

Arcot™ TransFort™

Issuer Software

**Operations Manual
Version 6.4.5**



455, West Maude Avenue, Sunnyvale, CA 94085-3517

TransFort Issuer Software—Operations Manual

Version 6.4.5

Publication Date: March 2008

Part Number: AT060-004DC-64000

Copyright © 2008 Arcot Systems, Inc. All rights reserved.

This manual, as well as the software described herein, is furnished under license and may be used or copied only in accordance with the terms of the license. The content of this manual is furnished for informational purposes only. It is subject to change without notice and should not be construed as a commitment by Arcot Systems.

Arcot Systems makes no warranty of any kind with regard to this manual. This includes, but is not limited to the implied warranties of merchantability, fitness for a particular purpose or non-infringement. Arcot Systems shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance or use of this material.

Except as permitted by the software license, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior written permission of Arcot Systems, Inc.

Trademarks

Arcot, the Arcot logo, WebFort, AccessFort, TransFort, ArcotID, and “Securing e-Business Anywhere” are all trademarks of Arcot Systems, Inc.

3-D Secure and Visa are trademarks of Visa International. SecureCode and MasterCard are trademarks of Mastercard International. Other trademarks are the property of their respective owners.

Patents

This software is protected by United States Patent No. 6,170,058, 6,209,102 and other patents pending.

Arcot Systems, Inc., 455, West Maude Avenue, Sunnyvale, CA 94085-3517.

Third Party Software

The following third-party software packages have been packaged with the TransFort Issuer Software:

libcurl

Copyright © 2000, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

OpenSSL

Copyright © 1998-2000 The OpenSSL Project. All rights reserved.

MSXML Parser 3.0

Copyright © 2000, Microsoft Corporation. All rights reserved.

Preface	1
About This Manual	2
Intended Audience	2
Information Included in this Manual	2
Related Publications	4
Conventions Used in This Book	5
 Introduction to 3-D Secure	 7
About 3-D Secure	8
3-D Secure Components	9
The Issuer Software	9
The Directory Server	10
The Merchant Software	10
3-D Secure Transactions	11
Enrollment Transactions	11
Cardholder Identity Verification Methods	13
Purchase Transactions	14
 Introduction to Issuer Software's Cardholder User Interface	 17
Cardholder User Interface for Enrollment	18
Enrollment Server URL	18
Identification Step	21
Terms and Conditions Step	21
Cardholder Verification Step (Attributes)	22
Cardholder Verification Step (Q&A)	23
Set Password	24
Set Personal Message	25
Account Management	26
Resetting Cardholder Password	26
Viewing Transaction History	28
Updating Cardholder Profile	29
Cancelling Enrollment	29
Merging of Enrollment Steps	30
Session Based ES	30
Cardholder Interface for Online Transactions	31
Selecting Locale During Activation During Shopping	31
ADS Pages	32
 Introduction to Administrator Operations	 33
Administrator Group Hierarchy	34
Master Administrators	34
Global Administrators	35
Issuer Administrators	35
Administrators	36

Privileges List	36
Advanced Authorization	40
Administrator Across Issuers	40
Administrator Across Levels	40
About Administrator Privileges and Password Policies	41
Dual Control	41
Administrator Password Policies	42
Getting Started with the Administrative Console	43
Administrative Console User Interface	43
Basic Administrator Tasks	45
Logging in and out of the Administrative Console	45
Changing your Administrator Password	46
Updating Your Profile	47
Exporting a Report to a File	48
Viewing the Exported File	49
Managing Administrators	51
Creating Administrator Accounts	52
Creating Administrators and Issuer Administrators	52
Creating Global Administrators	53
Creating Global Administrators using the DUC	54
Updating Administrator Privileges	56
Updating Administrator (CSR) and Issuer Administrator Privileges	56
Updating Global Administrator Privileges for a Selected Global Administrator	56
Enabling/Disabling Administrators	58
Resetting Administrator Passwords	59
Configuring Administrator Password Policy	60
Configuring Administrator Privileges	62
Master Administrator Operations	63
Managing Global Administrator Accounts	63
Viewing Administrator System Access Reports	65
CSR System Access Reports	65
Administrator Report Access Log	66
Administrator Activities Log	66
Issuer Administrator Account Reports	67
Issuer Administrator Report Access Log	67
Issuer Administrator Activities Log Report	68
Global Administrator Account Reports	68
Global Administrator Activities Log	68
Global Administrator Report Access Log	69
Administrator (CSR) Operations	71
About Cardholder Enrollment	72
Standard Enrollment	72

Verifying Cardholder Identity	72
Creating the Cardholder's Identifiers	72
Abridged Enrollment	73
Activation During Shopping (ADS)	73
Opt-In	74
Issuer Activation	74
Purchase Attempts	74
Managing Cardholder Accounts	75
Adding Cardholder Accounts	75
Viewing Cardholder Account Information	77
Updating the User ID	80
Locking/Unlocking Cardholder Accounts	81
Viewing the details of a particular cardholder's account	81
Updating Cardholder Enrollment Responses	82
Resetting a Cardholder's Password	83
Cancelling Cardholder Accounts	84
Receiving Promotional Emails	84
View/update Do Not Prompt	84
Changing the Locale of a Card	85
Issuer Administrator Operations	87
Configuring Issuer Parameters	88
Managing Administrators and Issuer Administrators	91
Managing Issuer Administrator Accounts	91
Managing Administrator (CSR) Accounts	91
Viewing Administrator System Access Reports	92
Report Codes	93
\$1Pre-Authorization Response Codes	94
AVS Result Codes	96
CVV/CVC2 Result Code	97
Cardholder Status Code	98
PARes Status Code	101
ECI Values	102
Invalid Request Codes	103
Reason Column Codes for Failed Transactions Report	104
Error Codes	107
Transaction Details Status Codes	108
Processing Errors	110
Glossary	115
Index	123

Preface

Welcome to the TransFort Issuer Software Operations Manual. This manual explains the 3-D Secure program (also known as SecureCode by MasterCard and Verified by Visa) and how it is implemented using the TransFort Issuer Software. This manual also provides instructions on system operations for Issuer Administrators and Administrators (CSRs).

About This Manual

This section describes the intended audience for this manual and lists the chapters included in the manual.

Intended Audience

This manual is intended for Customer Service Representatives (CSRs) responsible for managing 3-D Secure cardholder enrollment, and for Issuer Administrators responsible for managing Administrator (CSR) system accounts. If you are a Global or Master Administrator, you may want to refer to the *TransFort Issuer Software Administration Manual*.

Information Included in this Manual

This manual contains the following chapters:

- **Chapter 1, “Introduction to 3-D Secure”**, describes the 3-D Secure program, its components, types of transactions, and cardholder identity verification methods.
- **Chapter 2, “Introduction to Issuer Software’s Cardholder User Interface”** describes the cardholder user interface to the online authentication program. The chapter discusses the ES and ACS interface.
- **Chapter 3, “Introduction to Administrator Operations”**, describes the Administrator group hierarchy, administrator system access privileges, and instructions for using the Administrative Console.
- **Chapter 4, “Managing Administrators”** describes the different tasks to create and manage the all the different levels of administrators of Issuer Software
- **Chapter 5, “Administrator (CSR) Operations”**, describes cardholder enrollment in the 3-D Secure program and provides instructions on how to perform tasks specific to the Administrator group.
- **Chapter 6, “Issuer Administrator Operations”**, describes how to configure Issuer enrollment server information.
- **Appendix A, “Report Codes”**, contains tables that list the codes that appear on some of the administrator reports.

- [Appendix B, “Error Codes”](#), lists the error codes applicable to the Access Control Server (ACS) component of the Issuer Software.

Related Publications

This manual references the following documents:

<i>Transfort Data Upload Tool Installation and User Manual</i>	This manual contains instructions for installing and using the Transfort Data Upload Tool. The Transfort Data Upload Tool can be used to automatically upload certain cardholder data into the Issuer Software Database.
<i>TransFort Issuer Software Installation Manual</i>	This manual will guide the system administrator during the installation and configuration of the Issuer Software.
<i>TransFort Issuer Software Administration Manual</i>	This manual explains the 3-D Secure (also known as Verified by Visa or MasterCard's SecureCode) program and how it is implemented using the TransFort Issuer Software. This manual also provides instructions on system operations for all administrator levels and contains detailed system configuration information.

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Click the Add button. The changes will be added to the database.
<i>Italic</i>	Key Words	The <i>Messenger Service</i> must be started before the Web Server.
	Names of Publications	For more information, consult the <i>Administration Manual</i> .
	Emphasis	<i>Never</i> give anyone your PIN number.
Fixed-width	Command-line input or output	# <code>cd /opt/arcot</code>
	Code Samples	<code>./authproxy start</code>
	Text File Content	<code>[arcot/NetscapeCMS] host=tupelo.arcot.com endEntityPort=443 endEntityPortUsesSSL=0 agentPort=8100</code>
	File names	<code>arcot.ini</code>
<i>Italic fixed-width</i>	Variable text. Replace italic text with the appropriate substitution.	# <code>cd <i>install_directory</i> /Install.tgz</code>
	Variable portions of file names. Replace italic text with the appropriate substitution.	<code>init<i>ORACLE_SID</i>.ora</code>
Bold fixed-width	Emphasized code sample to highlight discussed topic.	<code>sub gatewayError { my (\$msg, \$errorCod) =@_ print"Content-type: text/html\n\n" ...</code>

Introduction to 3-D Secure

The Arcot TransFort Issuer Software fully implements the 3-D Secure online authentication program. 3-D Secure is an Internet-based service that provides cardholder authentication (or identification) during an online purchase transaction.

This chapter describes the following topics:

- [About 3-D Secure](#)
- [3-D Secure Components](#)
- [3-D Secure Transactions](#)

About 3-D Secure

In a real-world transaction, purchases require cardholders to actually present their payment cards to the merchant. The fact that a cardholder actually holds the card authenticates the cardholder. The merchant may read the magnetic stripe on the back of the card, and the cardholder may be asked to sign a receipt. These measures help reduce fraud. Criminals must actually steal a card in order to use it, and cardholders cannot easily deny purchases when their signature is on a charge receipt.

Internet purchases, however, only require the cardholder to supply the card number, the expiration date, and sometimes the billing address during a purchase transaction. As a result, fraud rates are much higher for Internet purchases than for real-world purchases. Criminals can obtain cardholder information, and cardholders can deny having made transactions (*friendly fraud*). Many cardholders are uncomfortable with this lack of security and do not make Internet purchases.

3-D Secure solves this problem by allowing each cardholder to create a secret password, known only to the cardholder, that is associated with the cardholder's account. This password is stored in the Issuer Software database. When shopping at a participating Internet merchant, the cardholder will be required to enter this secret password in order to complete a purchase.

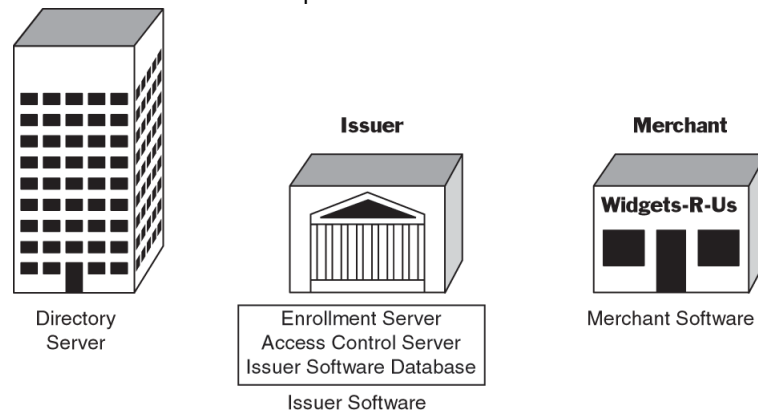
3-D Secure Components

The following components are required for a 3-D Secure transaction to take place. See [“3-D Secure Transactions” on page 11](#) for information on 3-D Secure transactions.

- The Issuer Software
- The Directory Server
- The Merchant Software

The following figure shows the location of each of these components in the 3-D Secure Authentication system.

Figure 1-1 The 3-D Secure Components



The Issuer Software

The Issuer Software, either maintained by an individual Issuer or by an **on-behalf-of host** (a third-party organization that hosts the Issuer Software for Issuers), is used to enroll cardholders in the 3-D Secure program and verify the identity of the cardholders attempting to make purchases from participating merchants. The Issuer Software is divided into three main components:

Table 1-1 Issuer Software Components

Component	Description
Enrollment Server (ES)	Enables cardholders to enroll in the 3-D Secure program and allows administrators to perform system operations through use of the Issuer Software Administrative Console.

Table 1-1 Issuer Software Components

Component	Description
Access Control Server (ACS)	Verifies the identity of cardholders during online purchase transactions.
Issuer Software Database	Contains the information used to enroll and authenticate cardholders participating in the 3-D Secure program.

The Directory Server

The Directory Server (DS) holds records of all card number ranges (but not cardholder-specific information such as cardholder name, and so on) that are participating in the 3-D Secure program. When a cardholder attempts a transaction at a participating merchant's site, the merchant contacts the Directory Server to determine the URL to the ACS used by the card's Issuer to verify the 3-D Secure transaction.

The Merchant Software

The Merchant Software is a collection of tools that the merchant uses to capture purchase requests, send authentication requests, receive and validate authentication responses, and record the transactions.

3-D Secure Transactions

There are two types of transactions between a cardholder and the Issuer Software:

- Enrollment Transactions
- Purchase Transactions

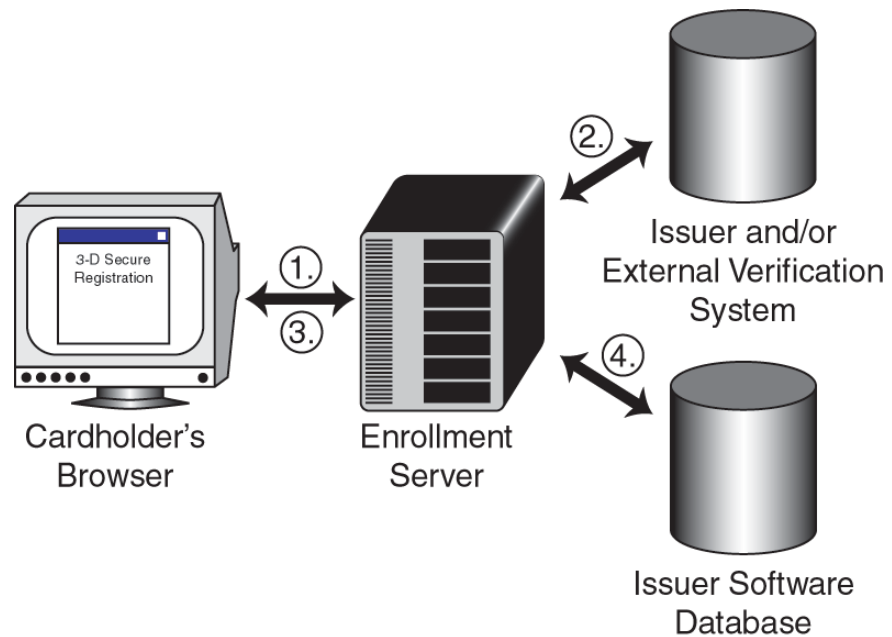
Enrollment Transactions

Cardholders must enroll in the 3-D Secure program before they can take advantage of 3-D Secure benefits. In order to enroll, cardholders access an Enrollment Web site hosted by their card Issuer. This Web site runs the Issuer Software Enrollment Server.

When a cardholder initiates an enrollment, the Enrollment Server opens a dialog with that cardholder. This dialog may involve several Web pages and can ask the cardholder a wide variety of questions. During this session, the cardholder will be asked to enter the card number, expiration date, and the cardholder's name. The cardholder may also be asked for other personal information such as the cardholder's social security number, mailing address, and so on. The Issuer Administrator configures the exact set of enrollment questions. The end result of this dialog is that the cardholder is identified, either by the Issuer Software itself or by an external verification system, and the cardholder is enrolled into the 3-D Secure program.

See [“Cardholder Identity Verification Methods” on page 13](#) for more information about enrollment screening.

[Figure 1-2](#) illustrates a standard 3-D Secure enrollment process:

Figure 1-2 3-D Secure Enrollment Process

The following are the steps involved in the enrollment process:

1. The cardholder accesses the card Issuer's Enrollment Web site and provides the required enrollment information.
2. The Issuer Software or external verification system uses the information to determine whether or not the cardholder is approved for enrollment.
3. If the cardholder is approved (in other words, the cardholder's identity is confirmed), the Issuer Software prompts the cardholder to enter a secret password and other configurable authentication information. This information is used to verify the cardholder's identity when the cardholder attempts to purchase an item online.
4. The Issuer Software processes the enrollment and records the cardholder information in the Issuer Software Database.

Issuers can choose to load certain cardholder enrollment data into the Issuer Software Database by using the Arcot Data Upload Tool for TransFort. The Data Upload Tool can load pre-enrollment data (such as cardholder telephone number, date of birth and so on) to use to authenticate enrollment, and post-enrollment data (such as password, personal message, and so on). See the *Arcot Data Upload Tool Installation and User Manual* for more information.

Cardholder Identity Verification Methods

The Issuer Software allows you to use any combination of the following identity verification options to authenticate cardholders during enrollment:

- Internal Verification
- \$1 Pre-Authorization
- External Verification

Internal Verification

Your financial institution may decide to verify the identities of cardholders who want to enroll in the 3-D Secure program by using several standard industry authentication questions. Standard industry questions include asking for the cardholder's home phone number, card billing address, and mother's maiden name. Typically, these questions are based on information that the Issuer already possesses.

The standard questions can be customized by the individual Issuer. The Global Administrator creates and updates the questions asked and also determines the number of questions that a cardholder must answer correctly.

For information on customizing these questions and determining the number of questions a cardholder must answer correctly, see the *Arcot TransFort Issuer Software Administration and Operations Manual*.

\$1 Pre-Authorization

MasterCard International's or Visa International's Pre-Authorization service determines the authentication status of a cardholder based on whether or not a test purchase in the amount of one dollar is authorized by the cardholder's account (it is only a test - no money changes hands). Together with other pre-authorization retrieval services, it verifies that the cardholder's account is valid and that the person initiating the transaction is the actual cardholder.

The Pre-Authorization service retrieves information about an account based on a requesting party's selection of Pre-Authorization retrieval services. A Pre-Authorization authentication request can be very simple or very complex, based on the number of Pre-Authorization retrieval services employed by the Issuer. The Issuer can employ one or many of the retrieval services when making an authentication request. The Issuer can also decide to use just the Pre-Authorization authentication service by itself, and employ none of the other retrieval services.

The following two Pre-Authorization retrieval services are available for identity verification during 3-D Secure enrollment:

- **AVS Authentication** - The Address Verification Service (AVS) determines the identity of a cardholder based on whether or not the cardholder correctly enters the card billing address when enrolling in the 3-D Secure program.
- **CVV2/CVC2 Authentication** - The Cardholder Verification Value 2 (CVV2) of Visa or the Card Validation Code 2 (CVC2) of MasterCard service determines the authentication status of a cardholder based on whether or not the cardholder correctly enters a three-digit verification code located on the signature panel on the back of the card.

The Global Administrator can specify the allowable AVS and CVV2/CVC2 return codes for the Issuer and the Issuer Administrator can configure the Issuer to enable the Pre-Authorization screening.

For information on how to enable Pre-Authorization and specifying the allowable AVS and CVV2/CVC2 return codes, see *Arcot TransFort Issuer Software Administration and Operations Manual*.

External Verification

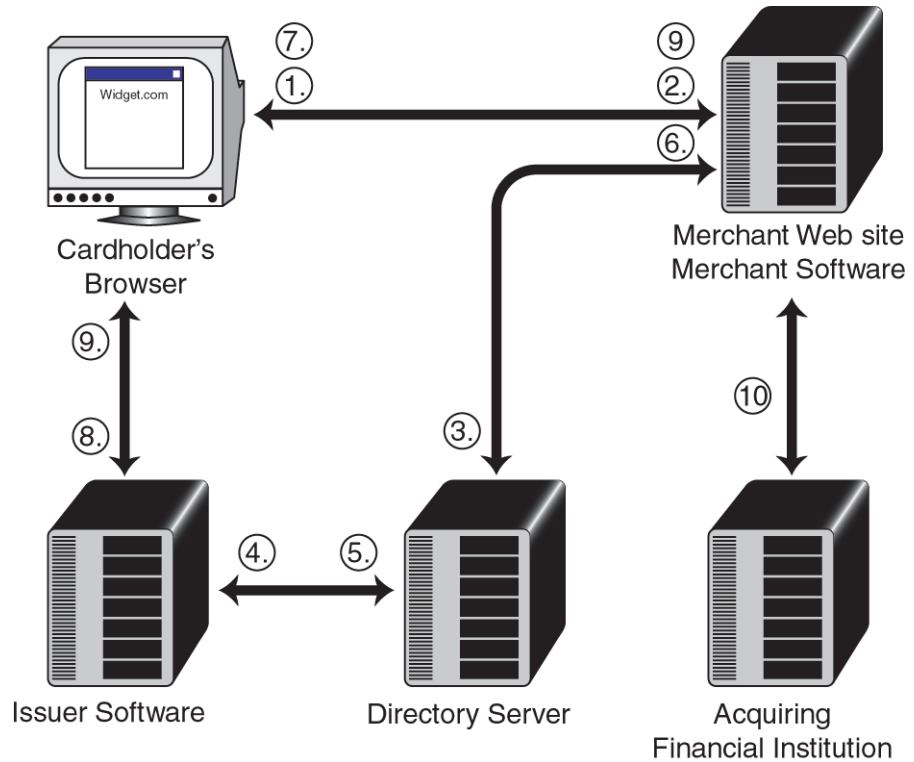
External verification is a real-time interface with an Issuer's own financial institution system. When a cardholder answers questions during enrollment, the Enrollment Server sends the cardholder's answers to this external system for verification. The external system invokes a verification program, verifies the cardholder answers, and sends the response back to the Enrollment Server.

The callouts feature in the system provides the functionality for external verification.

Purchase Transactions

When an enrolled cardholder visits a participating Internet merchant, the cardholder shops and checks out as normal. When the cardholder clicks on the final **Buy** button at the end of checkout, a popup window from the Issuer Software opens. This window asks the cardholder to enter the cardholder's secret password for identity verification. The cardholder enters the password, clicks **Submit**, and then completes the purchase.

The Issuer Software supports password-based, chip card-based, and ArcotID-based authentication. The following figure and process outline describe the password-based authentication:

Figure 1-3 3-D Secure Purchase Transaction Process

The following are the detailed steps involved in the purchase transaction process. This process assumes the cardholder's card number belongs to a participating card number range.

1. A cardholder accesses a Merchant Web site, selects items to purchase, and places them into a shopping cart.

At this point, the cardholder is ready to purchase the items.

2. The cardholder clicks the **Buy** button.

The merchant attempts to use 3-D Secure to verify the cardholder's enrollment status.

3. The Merchant Software forwards the message to verify the cardholder's enrollment status to the Directory Server.

4. The Directory Server forwards the message to the appropriate Issuer's installation of the Issuer Software.

The Issuer Software determines whether the cardholder is enrolled in the 3-D Secure program.

5. The Issuer Software sends a response back to the Directory Server specifying whether the cardholder is participating in the 3-D Secure program.

6. The Directory Server forwards this response back to the Merchant Software.

Embedded in this response is the URL of the Issuer Software server that will verify the identity of the cardholder.

7. If the cardholder is enrolled in the 3-D Secure Authentication program, a pop-up browser window from the Issuer Software appears to the cardholder and requests the cardholder's secret password for identity verification.

8. The cardholder enters the password and clicks **Submit**, which forwards the identity information to the Issuer Software.

The Issuer Software attempts to authenticate the cardholder.

9. The Issuer Software sends the Payer Authentication Response to the merchant through the cardholder's browser.

10. If the cardholder was authenticated, the merchant proceeds with the authorization exchange with the merchant's acquirer. If the cardholder was not authenticated, the merchant has the option to continue with or terminate the transaction.

Chapter 2

Introduction to Issuer Software's Cardholder User Interface

This chapter describes the following sections:

- [Cardholder User Interface for Enrollment](#)
- [Cardholder Interface for Online Transactions](#)

Cardholder User Interface for Enrollment

In order to enroll into the online payments authentication program, cardholders access an Enrollment Web site hosted by their card Issuer. The Enrollment Server running at this site provides an user interface to enable enrollment of the cardholder.

Enrollment Server URL

The URL to the ES website is provided by the Issuer. There can be a choice of ES URL's depending on the card range. In such a case, a *landing page* is provided to map the card number to the appropriate card range and corresponding template. This landing page can be used as a link in the Issuer web site to enable the cardholder to map to the correct enrollment page. When the cardholder enters the card number and clicks on the **Submit** button, the appropriate enrollment home page appears. See [Figure 2-2](#).

Figure 2-1 Landing Page for choosing ES URL

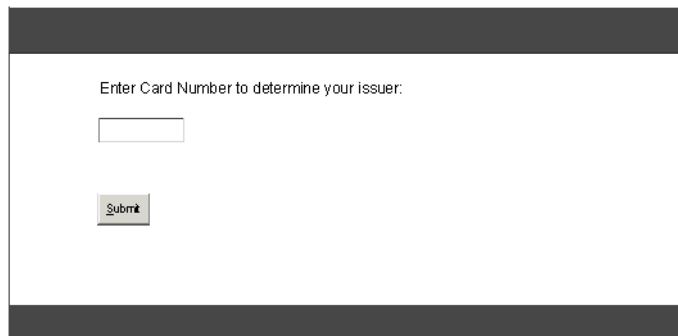
A screenshot of a web form titled "Enter Card Number to determine your issuer:". The form contains a single text input field for the card number and a "Submit" button below it. The entire form is enclosed in a white rectangular box with a thin black border, set against a dark gray background.

Figure 2-2 Enrollment Home Page


MEMBER BANK

Welcome | [Register Now](#) | [Account Assistant](#) | [Forgot your Password?](#) | [Contact Us](#) | [Help](#)

Account Assistant
Access a variety of features for quick and easy account management.

1. View the transaction history of your online purchases made using your password.
2. Create a new password.
3. Edit your account profile.
4. Enroll another card.
5. Cancel your enrollment.

Log in	Learn More	Extras
* indicates required fields User ID* OR Card Number* Your Name as it appears on card* First Name MI Last Name Forgot your Password? SUBMIT	Verified by VISA MasterCard. SecureCode. This is a place holder for Localized content from <enrollment folder>/18n/<locale>/index.jsp	This is a place holder for Localized content from <enrollment folder>/18n/<locale>/index2.jsp

[Welcome](#) | [Register Now](#) | [Account Assistant](#) | [Forgot your Password?](#) | [Contact Us](#)

If the issuer is not configured for User ID support the following screen is displayed:



Account Assistant

Access a variety of features for quick and easy account management.

1. View the transaction history of your online purchases made using your password.
2. Create a new password.
3. Edit your account profile.
4. Enroll another card.
5. Cancel your enrollment.

Log in	Learn More	Extras
* indicates required fields Card Number* Your Name as it appears on card* First Name MI Last Name Password* Forgot your Password? SUBMIT	Verified by VISA MasterCard SecureCode This is a place holder for Localized content from This is a place holder for Localized content from	This is a place holder for Localized content from <enrollment folder>/18n/<locale>/index2.jsp

[Welcome](#) | [Register Now](#) | [Account Assistant](#) | [Forgot your Password?](#) | [Contact Us](#)
[Help](#) | [Participating Merchants](#) | [About Us](#) | [Privacy Policy](#) | [Terms of Service](#)

The enrollment process is logically divided in the following steps:

- Identification Step
- Terms and Conditions Step
- Cardholder Verification Step (Attributes)
- Cardholder Verification Step (Q&A)
- Set Password
- Set Personal Message

The following sections describe each of the steps in more detail:

Identification Step

The cardholder at this stage has to choose between - *standard* or *abridged* type of enrollment. See *Arcot TransFort Issuer Software Administration and Operations Manual* for more information. The first step in both standard or abridged is the Identification Step, the cardholder should enter the card number in this step. This is a mandatory step.

Figure 2-3 Identification Step

The screenshot shows the 'MEMBER BANK' registration interface. At the top, there is a navigation bar with links: [Welcome](#) | [Register Now](#) | [Account Assistant](#) | [Forgot your Password?](#) | [Contact Us](#) | [Help](#). Below this, a banner area features a background image of a hand typing on a laptop and the text: 'Registration is easy. Just complete these quick steps and you will be ready to shop in a safer and more secure environment. All the information you enter is protected and will only be used to make sure of your identity and to make your online shopping safer. When you are done entering the requested information, just click the continue button on the bottom of each page.'

A progress bar indicates five steps: Step 1, Step 2, Step 3, Step 4, and Step 5. Step 1 is currently active and labeled 'Step 1 Register'. The main content area for Step 1 includes a note '* indicates required fields' and a text input field for 'Card Number *'. Below the input field are two buttons: 'CANCEL' and 'CONTINUE >'. On the right side of the page, there are logos for 'Verified by VISA', 'MasterCard SecureCode', and 'ARCOT processor logo'. At the bottom, a secondary navigation bar contains links: [Welcome](#) | [Register Now](#) | [Account Assistant](#) | [Forgot your Password?](#) | [Contact Us](#).

Terms and Conditions Step

The cardholder is optionally shown the “Terms and Conditions” of the online authentication program in the second step. This page is customized to display the Issuer’s terms and conditions for the program. The enrollment will proceed if the cardholder accepts the terms and conditions.

Figure 2-4 Terms and Conditions Page

The screenshot shows the 'MEMBER BANK' logo at the top left. A progress bar at the top indicates five steps, with 'Step 2' currently selected. On the left side of the page, a blue sidebar contains the text 'Step 2' and 'Terms of Service'. The main content area features a 'Verified by VISA MasterCard SecureCode' logo in the top right. Below this, a placeholder text reads: 'This is a place holder for Localized content from <enrollment folder>/i18n/<locale>/tandc.jsp'. At the bottom of the main area, there is an 'Accept' label next to a checked checkbox. Below the checkbox are three buttons: '< BACK', 'DECLINE', and 'ACCEPT'. The footer of the page includes the 'ARCOT' logo and a 'processor logo' placeholder.

Cardholder Verification Step (Attributes)

The cardholder is asked to enter personal information like name, date of birth User ID, etc., for identification in this step. The cardholder fields shown here are configurable. See the *Arcot TransFort Issuer Software Administration and Operations Manual* for more details.

NOTE:

An * next to the field name indicates that the information required for that field is mandatory.

Figure 2-5 Verifying Cardholder Attributes Step

MEMBER BANK

Step 1 Step 2 **Step 3** Step 4 Step 5

Step 3
Identify Yourself

Verified by VISA MasterCard SecureCode

Just fill in the information requested below and you'll be almost done with your Online Authentication Program registration. The information you provide is protected and will be used only to confirm your identity and make every online transaction safer. When you have filled in the information above, click on continue to proceed with your registration.

* indicates required fields

Your Name as it appears on card *
First Name MI Last Name

Email

< BACK CANCEL CONTINUE >

ARCOT processor logo

Cardholder Verification Step (Q&A)

The Issuer can configure a set of questions for the cardholder to answer in this step. Cardholder verification is done based on the responses to these questions. The questions appearing on this page can be configured. The questions can be in any of the locales supported by the Issuer. The cardholder can change the locale of the page by changing the query string in the URL. You must configure the questions for all the locales supported by the Issuer to enable this. See the *Arcot TransFort Issuer Software Administration and Operations Manual* for more details. The questions which requires a correct response from the cardholder has an * next to it.

WARNING

To view localized Issuer questions, the query string must be changed in the page previous to the questions page.

Figure 2-6 Issuer Questions page

The screenshot shows the 'MEMBER BANK' logo at the top left. A progress bar at the top indicates five steps, with 'Step 4' currently selected. On the left side of the main content area, 'Step 4' and 'Q & A' are displayed. On the right, there is a 'Verified by VISA MasterCard SecureCode' logo. Below this, a message states: 'For additional security, please answer the questions below. All information provided will be kept confidential.' A note indicates that an asterisk (*) denotes required fields. Two input fields are present: 'Mother's Maiden Name *' and 'Mailing Address 4 digit Zip Code *', both with masked text '****'. At the bottom right, there are three buttons: '< BACK', 'CANCEL', and 'CONTINUE >'. The bottom left corner features the 'ARCOT' logo and a 'processor logo'.

Set Password

The cardholder is verified and authenticated and then asked to create a User ID and password. This step is mandatory to complete enrollment. The password and the User ID is used to authenticate the cardholder during purchase transactions. Optionally a hint/response feature can be set in this page to be used when the cardholder forgets the password. See *Arcot TransFort Issuer Software Administration and Operations Manual* for more details.

NOTE: The card holder is asked to create an User ID provided the issuer is configured for User ID support.

Figure 2-7 Set Password Page

The screenshot shows the 'Set Password' page. On the left is a light blue sidebar with the title 'Set Password'. The main content area has a header '* indicates required fields'. Below this is the 'User ID' section with a text input field containing 'JeffSmith'. A paragraph explains that this enables a cardholder to login to the account assistant and update their profile. The 'Password' section follows, with a text input field containing '*****'. A paragraph explains that a password is required for online purchases and must conform to the policy. The 'Confirm Password' section has a text input field containing '*****'. A note specifies the password requirements: '4-10 characters, atleast-1 alphabets, atleast-1 numeric'. The 'Hint Question' section has a text input field containing 'Birth Place'. The 'Hint Answer' section has a text input field containing '*****'. The 'Confirm Answer' section has a text input field containing '*****'. At the bottom are three buttons: '< BACK', 'CANCEL', and 'CONTINUE >'. The footer contains the Arcot logo and the text 'processor login'.

Set Password

* indicates required fields

User ID

This enables a card holder to login to account assistant and update the profile and perform online transaction as well without having to use Cardnumber and Name

User ID*

Password

When you make a online purchase, you will be asked for your password. Your Online Authentication Program Password must conform to the password policy.

Password*

Confirm Password*

4-10 characters , atleast-1 alphabets , atleast-1 numeric .

If you've typed your password incorrectly or just plain forgotten it when making an online purchase, a window will pop up and give you the hint you supply here to help you remember the response you enter below.

Hint Question*

Hint Answer*

Confirm Answer*

< BACK CANCEL CONTINUE >

 processor login

Set Personal Message

The personal message can be set during enrollment. This message appears during a purchase transaction and offers the cardholder an assurance that the transaction is secure and valid.

Figure 2-8 Set Personal Message Page

MEMBER BANK

Step 1 Step 2 Step 3 Step 4 Step 5

Step 6
Set Password

Verified by VISA MasterCard SecureCode

Personal Message

As yet another security measure, we ask you to supply a Personal Message. When you see this message in the Online Authentication Program password window, that's your guarantee you are actually dealing with Online Authentication Program and not an impersonator. Your Personal Message must be from 1-30 characters.

If this card is held jointly, all the Personal Greetings will be displayed at the same time when shopping at a participating merchant.

Personal Message*

Thanks for your patience. Now just click the Submit button and allow about 2 seconds to receive your Online Authentication Program registration confirmation.

ARCOT processor logo

Account Management

The cardholder account can be viewed from the enrollment home page. The cardholder clicks on the **Account Assistant** link and is asked for the password. The account assistant allows the cardholder the following functions:

- Resetting Cardholder Password
- Transaction History
- Update Profile
- Cancel Enrollment

Resetting Cardholder Password

If the cardholder forgets the secret password or wants to change the password due to security reasons, the cardholder can reset or change the secret password from the *Account Assistant* link in the enrollment website. The Account Assistant requires the password to login. At the bottom of the password text boxes, there is a link “*Forgot Your Password?*” as shown in the [Figure 2-2](#).

IMPORTANT: The Issuer must configure the *Hint/response* feature or the *Issuer questions* feature to enable the cardholder to reset the password. When either of the features is not configured, the cardholder has to contact a CSR of the Issuer to reset the password.

When the cardholder clicks on this link, the actions which follow are explained below:

When the cardholder forgets the secret password or wants to change the password due to security reasons, the cardholder can reset or change the secret password from the *Account Assistant* link in the Issuer's enrollment website. The Account Assistant requires the password to login. See "[Account Management](#)" on page 26 for more details.

When the cardholder clicks on this link, the actions which follow are explained below:

1. If the Hint/Response for the password has been configured for the card range, and the Hint/Response information is available then the cardholder is shown the Hint/Response page.

See *Arcot TransFort Issuer Software Administration and Operations Manual* for information about configuring Hint/Response.

2. All the Hint questions for the card number are shown in a drop down box. The cardholder is asked to choose the hint question and provide the response in the text box.
3. If the cardholder is authenticated using the response and the response identifies the cardholder, the cardholder is shown the reset password page. The cardholder can reset the password and is automatically logged into the Account Assistant.
4. If the cardholder is authenticated, but the response does not identify any particular cardholder for the given card number, then a drop down box with all the names for the card number is displayed and the cardholder is asked to choose a name.

The selected cardholder is shown the reset password page. The cardholder can reset the password and is automatically logged into the Account Assistant.

5. If the Hint/Response feature is not enabled and if the Issuer Questions is configured for the card range, the cardholder is asked to enter the responses for the Issuer questions. The cardholder can change the locale from the query string to view localized Issuer questions.

NOTE: You have to configure the localized Issuer questions using the administrative console to enable this feature.

See the *Arcot TransFort Issuer Software Administration and Operations Manual* for more information about configuring Issuer questions.

6. If the cardholder is authenticated using the answers to identify the cardholder, the cardholder is shown the reset password page. The cardholder can reset the password and is automatically logged into the Account Assistant.
7. If the cardholder is authenticated, but the answers do not identify any particular cardholder for the given card number, then a drop down box with all the names for the card number is displayed and the cardholder is asked to choose a name.

The selected cardholder is shown the reset password page. The cardholder can reset the password and is automatically logged into the Account Assistant.

8. If both the Hint/Response and Issuer questions are not configured for the range then the cardholder sees a page informing the cardholder to contact a Customer Support Representative (CSR) to reset the password. Alternatively, the page can also have a link to a form to be filled and submitted to the Issuer online.

Viewing Transaction History

The cardholder can choose the start and end date to view the transaction history. The report generated can be sorted on any column like except the transaction amount.

Figure 2-9 Transaction History

MEMBER BANK

Welcome | Register Now | Account Assistant | Forgot your Password? | Contact Us | Help

Transaction History

Update Profile

Cancel Service

Logout

Verified by VISA MasterCard SecureCode

Transaction History:
The Transaction History below shows only online purchases using Online Authentication Program

A Transaction Record is generated each time your Password is entered into the pop-up box. As a result, your Transaction History may occasionally list purchases that have been subsequently cancelled, declined or refunded.

Start Date: April 15 2007

End Date: May 15 2007

SUBMIT

No transactions found 1

Cardholder Name	User ID	Amount	Merchant Name	Date of Purchase	Result
No transactions on this card					

Welcome | Register Now | Account Assistant | Forgot your Password? | Contact Us

Help | Participation Merchants | About Us | Privacy Policy | Terms of Service

NOTE: If the Issuer is not configured for User ID support, the User ID field is not displayed.

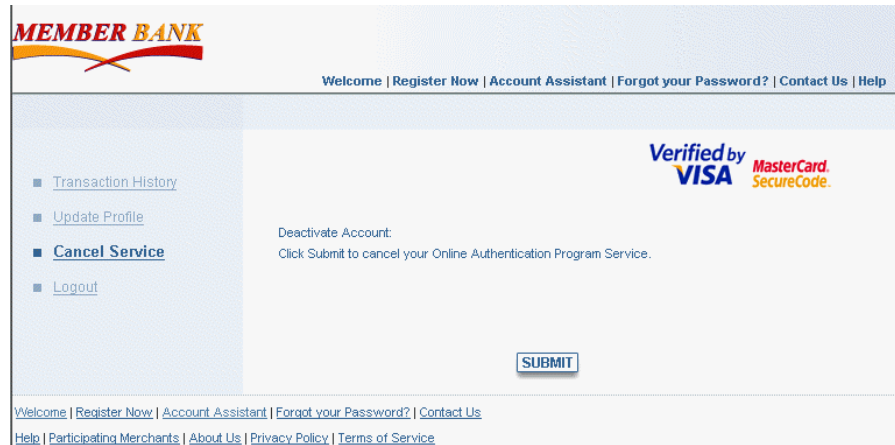
Updating Cardholder Profile

The cardholder can change the password, User ID, personal message and the preferred locale using the “*Change Your Profile*” link in the account assistant.

Figure 2-10 Change your profile page

Cancelling Enrollment

The cardholder can also cancel the enrollment into the program using the “Cancel Enrollment” link in the account assistant. On cancellation, the cardholder’s account will be deleted.

Figure 2-11 Cancel Enrollment

Merging of Enrollment Steps

Cardholder enrollment process can be combined into one or more steps. If the process is set to one page, the process of evaluation is from the top to the end of page the cardholder sees. The sequence of these steps can be configured. See *Arcot TransFort Issuer Software Administration and Operations Manual* for more details.

A step number decides the sequence of steps. The cardholder will see the enrollment screens in increasing order of the step number. More than one step can have the same step number and will be shown to the cardholder together. Alternatively the step can be disabled and will not appear during enrollment.

Session Based ES

Session states are stored in the new ES to minimize security breaches. This also allows cardholders to chase links (on the ES site) without fear of starting the enrollment all over again. This feature enables support for **Cancel** and **Back** buttons in the new ES for easy navigation by cardholder.

Cardholder Interface for Online Transactions

When an enrolled cardholder visits a participating Internet merchant, the cardholder shops and checks out as normal. The pop-up pages the cardholder views during the transaction are described below:

The cardholder clicks on the final Buy button at the end of checkout, a popup window from the Issuer Software opens. This window asks the cardholder to enter the cardholder's secret password for identity verification. This window also displays a Personal Assurance Message(PAM) that gives you assurance and you are confident that the purchases and payments you make on the are safe and secure.

Selecting Locale During Activation During Shopping

The pop-up page can optionally have a locale select drop-down menu. See [Figure 2-12](#). The cardholder can select the preferred locale from the menu. The system updates the cardholder profile to the selected locale. The new locale is automatically chosen the next time the cardholder sees the pop-up page.

Figure 2-12 Purchase Transaction page

Verified by Visa - Windows Internet Explorer
http://10.150.1.129/acspage/cap?RID=1&VAA=A

MEMBER BANK Verified by VISA

Protect Your Visa Card Online

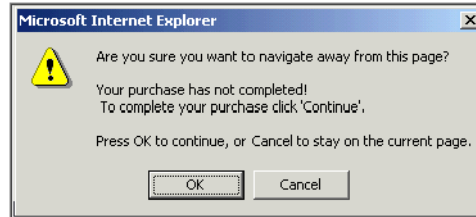
Your Visa Card has been pre-enrolled in Verified by Visa for added protection against fraud whenever your card is used at participating online stores--at no additional cost.

Merchant: Sample SDK Implementation
Amount: **USD 45.99**
Card number: XXXX XXXX XXXX 1004
Personal Message: Welcome
Last four digits of SSN:
Mothers maiden name:
Select Locale: English

The cardholder enters the password, clicks Submit, and then completes the purchase.

If the cardholder cancels the pop-up or closes the page, a warning is displayed. See [Figure 2-13](#).

Figure 2-13 Warning pop-up



ADS Pages

The ADS feature in TransFort enables the cardholder to enroll into the online authentication program during purchase transactions. If ADS is turned on, the cardholder sees a different set of pop-up pages. The pages which appear depend on the type of ADS configured.

See the *Arcot TransFort Issuer Software Administration Manual* for more information.

Introduction to Administrator Operations

The TransFort Issuer Software Administrative Console is a Web-based, operation and system management tool that provides a rich set of administrative functions including cardholder enrollment configuration, security policy configuration, Issuer Software configuration, and various report options. Different groups of administrators can access different functions.

This chapter discusses the following topics:

- Administrator groups and their relationships
- Advanced Authorization
- Administrator privileges and password policies
- Using the Administrative Console and performing basic administrator tasks

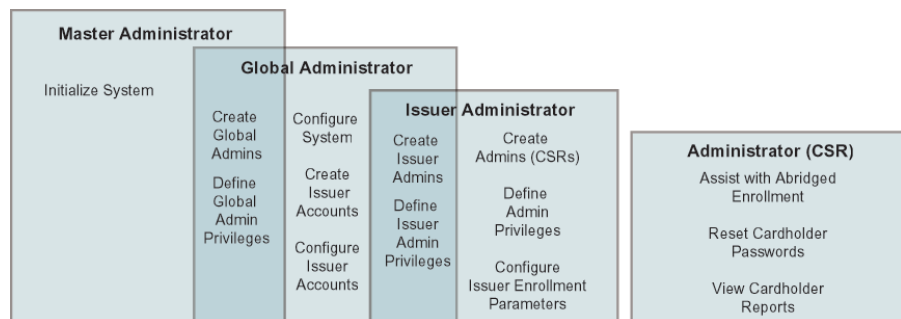
Administrator Group Hierarchy

The Issuer Software administrative functions have been distributed among four different groups of administrators. The four groups are:

- Master Administrator
- Global Administrator
- Issuer Administrator
- Administrator

This section describes each administrator role and the relationship between administrators. It also discusses Administrator privileges and password policies.

Figure 3-1 Administrator Hierarchy



Master Administrators

The Master Administrator is the highest level of administrator. The primary responsibilities of the Master Administrator are to initialize the system after installation, to create Global Administrator accounts, and to set the initial Global Administrator account access privileges.

When the Issuer Software is started for the first time after installation, two Master Administrator accounts are created to enforce dual control of the Master Administration functions. Both Master Administrators must be logged onto the system before the system will allow any changes. There will only be two Master Administrator accounts per installation (in other words, you cannot create additional Master Administrator accounts).

The list of privileges for a Master Administrator are:

- Create Global Administrator
- Configure Global Administrator Policy
- Configure Global Administrator Privileges

See [“About Administrator Privileges and Password Policies” on page 41](#) for more information on the dual control concept.

Global Administrators

Global Administrators are responsible for administering the Issuer Software. Tasks carried out by the Global Administrators include creating, managing, and modifying Issuer accounts; managing the Global, Issuer and CSR Administrator accounts; and maintaining and modifying the Issuer Software system configuration. Global Administrators can be assigned to one or more countries to provide country-specific administration support.

Master Administrators create the first Global Administrators when the Issuer Software is first set up. Other Global Administrator accounts can be created either by the Master Administrators or by Global Administrators who have been granted the privileges related to Global Administrator account creation.

Issuer Administrators

The primary responsibility of the Issuer Administrator is to manage the Administrator (CSR) accounts for an Issuer. This includes creating Administrator accounts and defining Administrator privileges. Issuer Administrators can also be responsible for managing other Issuer Administrator accounts and for configuring Issuer-specific enrollment parameters.

Global Administrators create the first Issuer Administrator accounts when the Issuer Software is first set up. Other Issuer Administrators can be created either by a Global Administrator or an Issuer Administrator granted the specific privileges related to Issuer Administration account creation.

See [Chapter 6, “Issuer Administrator Operations”](#) for detailed information on Issuer Administrator functions.

Administrators

Also known as Customer Support Representatives (CSRs), Administrators are responsible for the day-to-day operations related to cardholders who are enrolled or who are trying to enroll in the 3-D Secure program. For example, Administrators can assist with Abridged Enrollment, reset cardholder passwords, and view a variety of cardholder enrollment reports. For information on Abridged Enrollment, see “[Abridged Enrollment](#)” in [Chapter 5](#).

Administrator accounts are created by Issuer Administrators granted the specific privileges related to Administrator Account creation.

See [Chapter 5, “Administrator \(CSR\) Operations”](#) for detailed information on Administrator functions.

Privileges List

The privileges for all the administrators for the system are listed in the table below:

Table 3-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Configure Issuer Administrator Privileges	Update Issuer Administrator Privileges	Successful Registrations
Update Issuer Administrator Privileges	Reset Issuer Administrator Password	Reset Cardholder Password
View All Issuers	Reset Administrator Password	Update Cardholder Registration Data
Update FI Information	Enable/Disable Issuer Administrator Account	Lock/Unlock Cardholder
Global Administrator Activities Log	Configure Issuer Administrator Policy	Cancel 3-D Secure Service
Update ES Config	Create Issuer Administrator	Add Cardholder
Update ACS Config	Administrator Activities Log	Cardholder Account Inquiry
Add FI Information	Issuer Administrator Activities Log	Transaction Statistics
Create Issuer	Administrator Report Access Log	Registration Statistics
Reset Issuer Administrator Password	Issuer Administrator Report Access Log	Failed Transactions

Table 3-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Enable/Disable Issuer Administrator Account	Configure Issuer Parameters	Successful Transactions
Configure Issuer Administrator Policy	Configure Administrator Policy	Deactivated Cardholders
Create Issuer Administrator	Enable/Disable Administrator Account	Cardholders Added by Administrator
Reset Global Administrator Password	Update Administrator Privileges	All Registrations by Date
Enable/Disable Global Administrator Account	Create Administrator	Individual Registration Status
Update Global Administrator Privileges		Failed Registrations
Add Range Group		Upload Enrollment Data
Refresh ES/Administrator Cache		Upload Pre-Enrollment Data
Upload Enrollment Data		
Upload Pre-Enrollment Data		
Upload Admin Data		
Create Global Administrator		
Billing Information		
Update Issuer Callout		
Add Issuer Callout		
Update CallOut Configuration		
Add CallOut Configuration		
Verify Enrollment Log		
Update Issuer		
Add New Phone Support		
Add Issuer Customization		
Configure Administrator Privileges		
Reset Administrator Password		

Table 3-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Administrator Activities Log		
Administrator Report Access Log		
Successful Registrations		
Reset Cardholder Password		
Update Cardholder Registration Data		
Lock/Unlock Cardholder		
Cancel 3-D Secure Service		
Add Cardholder		
Cardholder Account Inquiry		
Issuer Administrator Activities Log		
Issuer Administrator Report Access Log		
Configure Issuer Parameters		
Configure Administrator Policy		
Enable/Disable Administrator Account		
Update Administrator Privileges		
Create Administrator		
Add/Update Issuer Questions		
Configure Enrollment Process		
Transaction Statistics		
Registration Statistics		
Failed Transactions		
Successful Transactions		
Deactivated Cardholders		

Table 3-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Cardholders Added by Administrator		
All Registrations by Date		
Individual Registration Status		
Failed Registrations		

Advanced Authorization

The hierarchical distribution of operations does not allow the administrators access across their fixed boundaries. Each level has a pre-defined privilege or role. The Advanced Authorization feature enables to create Global Administrators having all or any of the privileges of Global, Issuer and CSR administrators. Such *Enhanced Global Administrators* can perform any kind of administrative actions across Issuers without being tied down by the different levels in hierarchy. See the [Privileges List](#) for a details.

The following sections describe the different roles of the Enhanced Global Administrator:

Administrator Across Issuers

The Enhanced Global Administrator can be assigned a set of Issuers. This feature enables the administrator to operate across Issuers. There are two ways of associating an administrator with an Issuer:

1. **Creating an Global Administrator:** A list of Issuers is shown during the creation of global administrators. It is possible to select multiple Issuers. See [Chapter 4, "Creating Global Administrators" on page 53](#) for detailed instructions. The administrator thus created can operate on all the Issuers selected during creation.
2. **Creating an Issuer:** A list of all existing Global Administrators is shown when an Issuer is created. All the administrators selected and the administrator creating the Issuer will have control over the new Issuer. See [Chapter 5, "Administrator \(CSR\) Operations" on page 71](#) for detailed instructions.

An Enhanced Global Administrator should choose from a list of Issuers to do any Issuer specific operations.

Administrator Across Levels

An Enhanced Global Administrator can be defined during creation of an Global Administrator. The privilege list shown here includes the privileges of both the Issuer Administrators and Administrators (CSR's). Selecting all the privileges will enable the enhanced global administrator to perform all operations across levels.

About Administrator Privileges and Password Policies

Each administrator group has a different set of privileges. For purposes of this discussion, **privileges** are the tasks that an administrator is allowed to perform in the Administrative Console. The privileges are defined when during creation of an administrator. A global administrator defines administrator privileges and whether the tasks require dual control for Issuer administrators and Administrators (CSRs). Each administrator group (except CSRs) can set password policies for their own group and the next lower level administrator group.

The following sections describes the administrator dual control concept and administrator password and authentication policies.

Dual Control

Depending on the Issuer or processor's production policy, certain administrative tasks may require dual control. **Dual control** requires two administrators with appropriate privileges to log into the system at the same console in order to proceed with the task. Dual control stays on for the session till the second administrator explicitly logs out. The Administrative Console menu displays an asterisk (*) next to tasks that require dual control.

Master Administrators or Global Administrators with the appropriate privileges can specify dual control for specific tasks on the applicable administrator privileges pages.

NOTE:

An Enhanced Global Administrator will not require dual control for Issuer and CSR administrator privileges requiring dual control.

For information on how a Global Administrator can specify dual control, see [Chapter 4, "Configuring Administrator Privileges"](#) on page 62

For information on how a Master Administrator can specify dual control, see "[Master Administrator Operations](#)" in [Chapter 4](#).

Administrator Password Policies

Administrator password policies provide additional security protection for the administrative operations. The different levels of Administrators have jurisdiction over the next lower level administrator accounts in terms of setting password policy. For example, Issuer Administrators set the password policies for Administrators (CSRs). Configurable password policy options include password length, password format, number of failed login attempts allowed, and renewal frequency.

For information on how an Issuer Administrator can set password policy for Administrators and Issuer Administrators, see [Chapter 6, “Issuer Administrator Operations”](#).

For information on how a Global Administrator can set password policy for Issuer Administrators and other Global Administrators, see [Chapter 4, “Configuring Administrator Password Policy”](#) on page 60.

For information on how a Master Administrator can set password policy for Global Administrators, see [Chapter 4, “Master Administrator Operations”](#) on page 63.

Getting Started with the Administrative Console

This section describes the Administrative Console user interface and basic Administrator tasks that are universal to all Administrator groups.

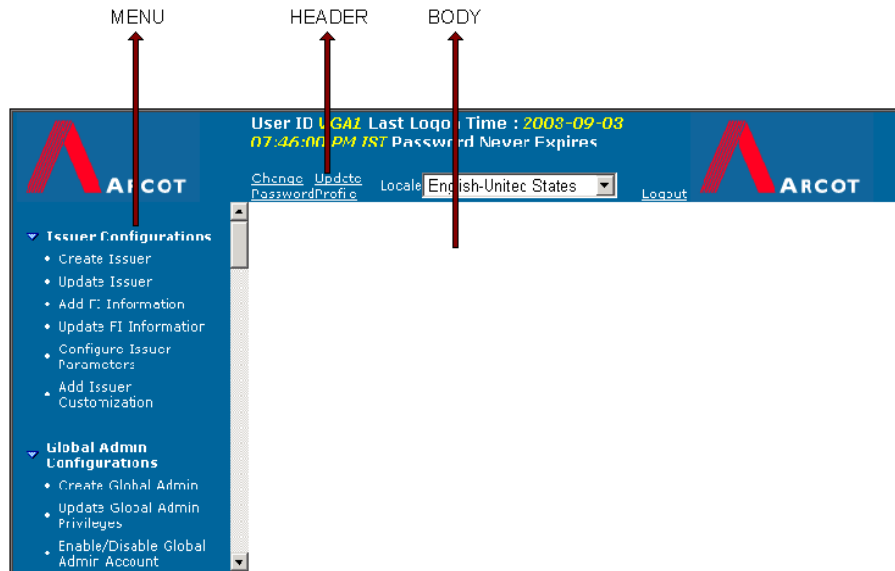
Administrative Console User Interface

The Administrative Console used by all Administrator groups has the same user interface. The user interface is composed of a three-framed view:

Table 3-2 Administrative Console User Interface

Frame	Description
Header	Displays branding logos, logon information, and links to administrator-specific tasks. The login information includes the User ID of the administrator who is currently logged on, the time the logon occurred, and the number of days in which the administrator's password will expire. The header also displays a field labelled Locale which contains the preferred language of the administrator. Use the drop down menu to select the preferred locale. Additionally, if a second administrator is logged on (for tasks requiring dual control), the second administrator's User ID is displayed in a field called Secondary User ID.
Menu	Displays the action and report menu links (or privileges) available for the current administrator.
Body	Displays the task page for the selected menu option.

The following figure diagrams the placement of the frames.

Figure 3-2 Administrator Interface Layout and Components

The Administrative Console uses the following navigation conventions:

Table 3-3 Administrative Console Navigation Conventions

Link or Button	Function	Location of Link or Button
Cancel	Cancels any user input and displays a blank body page.	Located in the Body frame of applicable function pages.
Export	Displays a “Save As” window that allows you to export report data in Comma Separated Value (CSV) format. See “Exporting a Report to a File” on page 48 for further information on this feature.	Located in the Body frame of applicable report pages.
[<<Previous] 1 2 3 [Next>>]	Scrolls through different pages of an online report.	Located on the left side immediately above and beneath the contents of a report.
Submit	Processes the current task or displays the information you are requesting.	Located in the Body frame of applicable function pages.

Basic Administrator Tasks

All Administrator groups, except where indicated, can perform the following Administrator-specific tasks:

- Log in and out of the Administrative Console.
- Change your Administrator Password
- Update your Profile*
- Export a report to a file*

The following sections provides instructions on how to perform these tasks.

Logging in and out of the Administrative Console

The following procedures describes how to log in and out of the Administrative Console. Obtain the applicable administrator URL from your Global Administrator or other system administrator prior to performing this procedure.

To log in to the Administrative Console (all administrators except Master Administrators):

1. Open a Web browser.
2. Enter the applicable Administrative Console **URL**.

The default Administrative Console URL for Administrators (CSRs) and Issuer Administrators is:

```
https://<%machine_name%>/vpas/admin/adminlogin.jsp?bank=IssuerDir
```

Where the *IssuerDir* is the name of the Issuer account folder created by the Global Administrator when setting up the Issuer account. For more information, contact the Global Administrator responsible for managing the Issuer Software.

The default Administrative Console URL for Global Administrators is:

```
https://<%machine_name%>/vpas/admin/adminlogin.jsp
```

The applicable *Administrator Login* page appears.

3. Type your Administrator **User ID** and **Password** in the applicable fields and click **Submit**.

The initial Administrative Console page appears.

**.Master Administrators do not have access to any reports in the system. Hence they cannot configure any report profiles.*

To log in to the Administrative Console (Master Administrators only):

1. On the Windows **Start** menu of the designated local Master Administrator machine, choose **Programs | TransFort Admin | Master Admin Login**.

NOTE:

Master Administrators are restricted to logging in to the Administrative Console from the machine on which the ES & Admin Console is installed. Arcot recommends using Arcot WebFort to enable remote login.

The *Master Administrator Login* page appears. This login requires both Master Administrators to be present.

2. Enter the **first Master Administrator password** in the applicable field, then have the second Master Administrator enter the **second Master Administrator password** in the applicable field.
3. Click **Submit**.

The initial Administrative Console page appears.

To log out of the Administrative Console:

- In the Administrative Console, click the **Logout** link located in the upper-right corner of the Header frame.

The system logs you out and displays the *Administrator Login* page.

NOTE:

If two administrators are logged on for tasks that require dual control, the secondary administrator should logout via the **Logout Secondary** link when the task is completed. Otherwise, the secondary administrator remains logged on until the first administrator logs out.

Changing your Administrator Password

Upon logging in to the Administrative Console for the first time, you may be required to change your password. Additionally, your administrator account may have been set up so that your password expires after a specific time interval (for example, every 60 days). In these cases, you will need to change your password when prompted. Otherwise, you may change your password as desired. The password must conform to the password policy defined. See “[Configuring Administrator Password Policy](#)” on page 60 in [Chapter 4](#) for more information

To change your Administrator password:

1. In the Administrative Console, click the **Change Password** link located in the Header frame.

The *Change Password* page appears.

2. Type the new **password** in the applicable fields and click **Submit**.

The system changes your password. The next time you log on to the Administrative Console, you will use this new password.

Updating Your Profile

Each administrator has a profile that specifies the preferred locale, number of records to be shown per report page as well as the default start date the system will initially choose in the report query pages. You may modify your profile as desired.

To update your profile:

1. In the Administrative Console, click the **Update Profile** link located in the Header frame.

The *Update Your Profile* page appears.

2. Type the **Records per page** and **Start date offset** information in the applicable fields. Select **Locale**, **Local Time Zone** and **Date Order for Report Generation** from the drop down menus and click **Submit**.

The following table provides information on the fields on the *Update Your Profile* page.

Table 3-4 Update Profile Page Fields

Field	Description
Records Per Page	The maximum number of records that the system will display on a report page. If you select --, Records Per Page defaults to a value set by the Issuer.
Start date offset	The offset from the query date that the system will use by default. You can choose two different types of offsets: First day of the current month If chosen, by default the query range will start on the first day of the month and go through the day of the query. Number of days offset If you specify an integer value, the query range will start the specified number of days prior to the day of the query and go through the day of query.

Table 3-4 Update Profile Page Fields

Field	Description
Locale	The preferred language of operation of the administrator. Select one of the languages from the drop-down menu.
Local Time Zone	The preferred time zone of the Issuer. This is the time zone used in reports.
Date Order for Report Generation	Display order for date input field for administrative reports. This parameter determines the input date format for search criterion used in administrative reports.

NOTE:

The administrator can set the locale from the drop-down menu in the header of the Administrative Console. This changes the locale only for that particular session. To set locale across sessions, change it using the *Update Your Profile* link.

The message “Admin Profile Updated Successfully” appears on the page.

Exporting a Report to a File

Every administrator report includes an option to export a report to a Comma Separated Value (CSV) file. You can then open these reports in another software application and manipulate the data as desired. This is the recommended method if any kind of post processing sorting is required for the reports.

To export a report to a file:

1. Click the desired report link.
The selected report page appears.
2. Type the report criteria in the applicable fields and click the **Export** button.
A *Save As* dialog box appears.
3. Select the directory in which to save the file, rename the file as desired, and click **Save**.

The system saves the file to the selected directory.

IMPORTANT:

Save the file as a .txt file instead of the default .csv extension. Follow the steps described below to ensure a successful export.

Viewing the Exported File

To view the exported file in Microsoft Excel:

1. Choose **File | Open**.

The *Open* dialog box appears.

2. Locate the .txt file you want to open, click on it to select it, and click **Open**.

The *Text Import Wizard* appears.

3. Click **Next** on the *Step 1 of 3* page without changing the default choices.

The *Step 2 of 3* page appears.

4. Under **Delimiters**, de-select **Tab**, select **Comma**, and then click **Next**.

The *Step 3 of 3* page appears.

5. Change the default data format for column(s) containing large numbers (for example, a PAN column) by selecting the particular column in the **Data preview** window and selecting **Text** under **Column data format**.

6. When you have completed the column data format changes, click **Finish**.

The report appears as an Excel spreadsheet.

Chapter 4

Managing Administrators

The Issuer Software administrative functions are distributed among four different groups of administrators. See “[Administrator Group Hierarchy](#)” on page 34 for more information regarding the groups and their relationship. This chapter discusses how to create and manage the administrators.

The chapter describes the following tasks needed to manage the administrators:

- [Creating Administrator Accounts](#)
- [Updating Administrator Privileges](#)
- [Enabling/Disabling Administrators](#)
- [Resetting Administrator Passwords](#)
- [Configuring Administrator Password Policy](#)
- [Configuring Administrator Privileges](#)
- [Master Administrator Operations](#)
- [Viewing Administrator System Access Reports](#)

NOTE:

This chapter describes all possible administrator related tasks. Whether you have the authority to complete the tasks described is defined by a higher level administrator.

NOTE:

With appropriate privileges, every group of administrators (except CSR's) can manage their own group and the next lower level administrator group.

Creating Administrator Accounts

Issuer Administrators are responsible for creating the Administrator (CSR) accounts and other Issuer Administrators for each Issuer.

Global Administrators are responsible for creating other Global Administrators. Master Administrators can also create Global Administrators. The following sections provide instructions on creating different type of administrator accounts:

NOTE:

Depending on your Issuer Administrator privileges configuration, some of these tasks may require dual control. See [“Dual Control” on page 41](#) for information on this concept.

Creating Administrators and Issuer Administrators

When you create an Administrator account, you define a User ID and temporary password for the Administrator. You can also adjust the default Administrator privileges for the particular Administrator.

To create CSR or Issuer Administrator accounts:

1. Click one of the following links:
 - For CSR accounts, choose the **Create Administrator** link.
 - For Issuer Administrator accounts, choose the **Create Issuer Administrator** link.

The appropriate page appears.

2. Select the applicable **Issuer**, type the desired **User ID** and **password** in the applicable fields.

NOTE:

The User ID must be a single character string. In other words, do not put a space in between words. Incorrect: M Smith. Correct: MSmith.

3. You can specify whether the Administrator must:
 - a. *Change Password at first login*

- b. Password never expires.*

You can select the check boxes provided for these options.

You can consider selecting the Password Never Expires option for administrators who are given Upload privileges.

4. If desired, select or clear any **Action and Report Privileges** to which you do not wish this Administrator to have access.
5. Click **Submit**.

The message “Admin Created Successfully” appears.

Creating Global Administrators

Global Administrators can be responsible for creating and managing other Global Administrator accounts. You can adjust the privileges for individual Global Administrator accounts based on the default privileges set for Global Administrators by your Master Administrators.

For information configuring Global Administrator privileges by a Master Administrator, see “[Configuring Administrator Privileges](#)” on page 62.

When you create a Global Administrator account, you define a User ID and temporary password for the Global Administrator, as well as specifying the countries over which the Global Administrator will have control. You can also adjust the default Global Administrator privileges for the particular Global Administrator and define the list of Issuers the Global Administrator can support.

To create a Global Administrator account:

1. Click the **Create Global Admin** link.

The *Create Global Administrator* page appears.

2. Type the desired **User ID** and **password** in the applicable fields.
3. You can specify whether the Administrator must:
 - a. Change Password at first login*
 - b. Password never expires.*

You can select the check boxes provided for these options.

You can consider selecting the Password Never Expires option for administrators who are given Upload privileges.

4. To add a country over which the Global Administrator will have control, scroll through the **List of Countries** and select a **country**, then click >>>> to add the country to the **Selected Countries** box. To select multiple countries, press and hold **Ctrl** while selecting the desired countries and then click >>>>.

The **List of Countries** box only displays the countries over which you (and the other logged on Global Administrator, if dual control was enforced) have control.

To de-select a selected country, select the **country** in the **Selected Countries** box and click <<<<.

5. To add an Issuer over which the Global Administrator will have control, scroll through the **List of Issuers** and select an **Issuer**, then click >>>> to add the Issuer to the **Selected Issuers** box. To select multiple issuers, press and hold **Ctrl** while selecting the desired issuers and then click >>>>.

The **List of Issuers** box only displays the countries over which you (and the other logged on Global Administrator, if dual control was enforced) have control.

To de-select a selected issuer, select the **Issuer** in the **Selected Issuers** box and click <<<<.

6. If desired, de-select any **Action and Report Privileges** to which you do not wish this Global Administrator to have access.
7. Click **Submit**.

The message “Admin Created Successfully” appears.

Creating Global Administrators using the DUC

You can easily create and update Global Administrators using the Data Upload Client. This feature allows you to add or update a global administrator based on an existing model administrator. To add a new administrator the upload administrator uses the model admin to copy privileges, attributes and states to the new administrator and populates only specific unique requirements like userid and password. This utility improves productivity, ensures consistent definitions and ultimately reduces errors. See the *Arcot Data Upload Tool Installation and User Manual* for more details on how to use this feature.

The Master Administrator can create the Global administrator with the *Upload Admin Data* privilege. Global administrators having this privilege can create or update other global administrators using the DUC. They can also pass this privilege to the new administrators created.

Arcot recommends that you create the initial model administrator with necessary precautions. The new administrator created will have all the privileges, Issuer associations, state and any other attributes of the model administrator. If you update existing administrators, irrespective of whatever the current privileges, the administrators will get updated to the same attributes of the model administrator.

Arcot specifically recommends that you select the *Change password at first logon* option for the model administrator. The password policy is enforced on the newly created administrators. Arcot also strongly recommends that model administrator is not used to login to the console and perform any administrative operations. This will impact the state of the model administrator and any new administrators created or updated using DUC will get impacted. For example, at first login, the model administrator is asked to change password and this attribute is passed on to the other administrators created later.

Figure 4-1 Creating Model Global Administrator

Create Global Administrator

User ID, Password, select a list of countries for this administrator, check the appropriate privileges and it.

User ID	JohnSmith
Password	*****
Re-type Password	*****
☒ Admin must change password at first login	
☐ Password Never Expires	

List Of Countries - United Kingdom - United States - Uruguay - Uzbekistan	>>>> <<<<	Selected Countries - United Kingdom - United States
List Of Issuers - Citibank - Citibank1 - Citibank2 - foram	>>>> <<<<	Selected Issuers Citibank

Updating Administrator Privileges

This function lets you adjust the privileges for an existing Administrator account.

Updating Administrator (CSR) and Issuer Administrator Privileges

To update Administrator privileges:

1. Click the **Update Administrator Privileges** link or the **Update Issuer Admin Privileges** link.

The *Update Issuer Administrator Privileges* or *Update Administrator Privileges* page appears.

2. Use the drop-down menu to select the desired Issuer.

A **User ID** field appears.

3. Use the drop-down menu to select the desired **User ID**.

The system displays a list of all possible **Action & Report Privileges** for an Administrator account.

4. Modify the privileges as desired.

5. Click **Submit**.

The message “Admin Profile Updated Successfully” appears.

This function lets you adjust the privileges for an existing Issuer Administrator account. The privileges correspond to menu links available to the Issuer Administrator.

Updating Global Administrator Privileges for a Selected Global Administrator

This function lets you adjust the privileges for an existing Global Administrator account. The privileges correspond to menu links available to the Global Administrator.

To update Global Administrator privileges:

1. Click the **Update Global Admin Privileges** link.

The *Update Global Administrator Privileges* page appears.

2. Use the drop-down menu to select the desired **User ID**.

The system displays a **List of Issuers** and a list of all possible **Action & Report Privileges** Global Administrator account.

3. Modify the list of issuers as desired.
4. Modify the privileges as desired.
5. Click **Submit**.

The message “Admin Profile Updated Successfully” appears.

Enabling/Disabling Administrators

There may be times when you need to disable an existing Administrator account (for example, an Administrator might be leaving the company or going on an extended leave of absence). Disabling an account locks that Administrator out of the system. Alternatively, there are times when you may need to enable a locked account (for example, when an Administrator returns from an extended leave of absence).

To enable or disable an Administrator account:

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Enable/Disable Issuer Admin Account**
 - For CSR's choose, **Enable/Disable Administrator Account**
 - For Global Administrators choose, **Enable/Disable Global Admin Account**

The appropriate page appears.

2. Use the drop-down menu to select the applicable **Issuer**.

The system displays a **User ID** field.

3. Use the drop-down menu to select the desired **User ID**.

The system displays the **Status** and **Remarks** fields.

4. Do one of the following:
 - a. To disable an Issuer Administrator, use the **Status** drop-down menu to select **Locked**.
 - b. To enable an Issuer Administrator, use the **Status** drop-down menu to select **Active**.
5. Type any **remarks** concerning the status change in the **Remarks** field.
6. Click **Submit**.

The message "Issuer Administrator Account Locked/Unlocked Successfully" appears.

Resetting Administrator Passwords

You can reset passwords for Administrators who forget their passwords. The new password should adhere to the password policy applicable to this Administrator. See [“Configuring Administrator Password Policy,”](#) for more information.

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Reset Issuer Admin Password.**
 - For CSR’s choose, **Reset Administrator Password**
 - For Global Administrators choose, **Reset Global Admin Password**

The appropriate page appears.

2. Use the drop-down menu to select the applicable **Issuer**.

The system displays a **User ID** field.

3. Use the drop-down menu to select the desired **User ID**.

The system displays the **New Password**, **Re-Type Password** and **Remarks** fields.

4. Type the **new password** and any **remarks** in the applicable fields and click **Submit**.

The message “Admin Password Modified Successfully” appears.

Configuring Administrator Password Policy

This function lets you configure password restrictions for the Administrators and Issuer Administrators accounts for a specific Issuer. The Master Administrator configures the password policy for all the Global administrators in the system. If you change this policy once it is in place, the new policy will only affect new Administrators or Administrators that change their passwords after the updated policy is in place. It will not affect the existing Administrator passwords.

To configure Administrator password policy:

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Configure Issuer Admin Policy**.
 - For CSR's choose, **Configure Administrator Policy**
 - For Global Administrators choose, **Configure Global Admin Policy**.

The appropriate page appears.

2. For the CSR's and Issuer Administrators, use the drop-down menu to select the desired **Issuer**.

The system displays the list of configurable password policy options.

3. Specify the desired values in the applicable fields.

The following table describes the Administrator password policy parameters. To disable a particular option, specify "--" in a drop-down list or leave a text field blank.

Table 4-1 Administrator Password Policy Parameters

Parameter	Description
Issuer	The Issuer to which these parameters will be applied.
Failed Login Attempts Allowed - Per Session	The number of times an incorrect login attempt may occur consecutively during a single session.
Failed Login Attempts Allowed - Across Sessions	The number of times an incorrect login attempt may occur consecutively across multiple sessions.
Password Length - Minimum	The minimum number of characters that a password must have to be valid.
Password Length - Maximum	The maximum number of characters that a password may have to be valid.

Table 4-1 Administrator Password Policy Parameters

Parameter	Description
Password Format Restriction - Minimum Numeric	The minimum number of numeric characters that must be used in the password.
Password Format Restriction - Minimum Alphabets	The minimum number of alphabetic characters that must be used in the password.
Password Format Restriction- Minimum Special Characters	The minimum number of special characters that must be used in the cardholder's secret password. Special characters supported are: ! " # \$ % & ' () * + , - . / ; < = > ? @ .
Password Renewal frequency	The maximum number of days that a password will remain valid before it must be changed.
Maximum Inactivity Period	The maximum number of days that an account may be inactive before the account is suspended.
Allow admin to reset password after expiry	If you select this check box, you can allow the administrators to reset their password after a lockout due to password expiration or administrator inactivity.

4. When you have completed your modifications, click **Submit**.

The message “Admin Configuration Params Updated Successfully” appears.

Configuring Administrator Privileges

This function lets you define a default set of privileges to use for all Administrators. The privileges correspond to the menu links that are displayed for the Administrator accounts.

NOTE:

Only a Global Administrator can configure the privileges of all the CSRs and Issuer Administrators. The Master Administrators can configure the privileges for all the Global administrators in the system.

To configure Administrator privileges:

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Configure Issuer Admin Privileges**.
 - For CSR's choose, **Configure Administrator Privileges**
 - For Global Administrators choose, **Configure Global Administrator Privileges**.

The appropriate page appears. This page lists all of the possible Administrator menu options and indicates whether the option is a report or an action and whether the option requires dual control.

2. Use the **Enable** check box to specify an option as enabled and the **Dual Control** check box to specify an option as requiring dual control.

See **“Dual Control” on page 41** for information on the dual control concept.

3. When you have completed configuring the privileges, click **Submit**.

The message “Admin Privileges Updated Successfully” appears.

Master Administrator Operations

When the Issuer Software is installed, the installation process creates two Master Administrator accounts. There will only be two Master Administrator accounts per Issuer Software deployment.

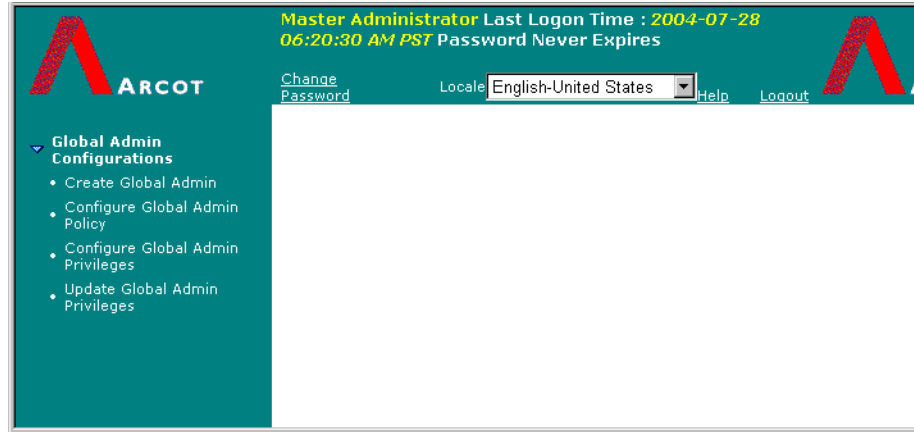
The primary responsibility of the Master Administrators is to create Global Administrator accounts and define the Global Administrator account access privileges. This section provides instructions for the tasks related to managing Global Administrator accounts.

Managing Global Administrator Accounts

Both Master Administrators must be present and enter their separate passwords before they can perform any Global Administrator account management tasks. See [“Logging in and out of the Administrative Console” on page 45](#) for detailed instructions on Master Administrator login.

Master Administrators can perform the following tasks:

- Create Global Administrator accounts. See [“Creating Global Administrators,”](#) for detailed instructions.
- Configure Global Administrator password policy. See [“Configuring Administrator Password Policy,”](#) for detailed instructions.
- Configure Global Administrator privileges. See [“Configuring Administrator Privileges,”](#) for detailed instructions.
- Update Global Administrator privileges. See [“Updating Administrator Privileges,”](#) for detailed instructions.

Figure 4-2 Master Administrator Page

Viewing Administrator System Access Reports

All the administrator access to the Issuer Software system are recorded in two types of logs:

- Activities Log
- Report Access Log

The Issuer Administrator can view these reports to retrieve and display information about Administrators (CSRs) and Issuer Administrators system use. The Global Administrator can view the system access reports for CSRs, Issuer Administrators and Global Administrators.

You can choose to view a report online or export a report to a file to use in another software program.

NOTE:

This section provides instructions on how to view reports online. See [“Exporting a Report to a File” on page 48](#) for instructions on how to export a report.

The system displays reports according to the information set up in your Report Profile. See the [“Updating Your Profile” on page 47](#) for information on how to change your Report Profile.

The reports according to the administration level fall into the following categories:

- [CSR System Access Reports](#)
- [Issuer Administrator Account Reports](#)
- Global Administrator Account Reports

This section describes the information contained in each report and provides instructions on how to access and view each report.

CSR System Access Reports

There are two reports that display information about Administrator (CSR) system access:

- [Administrator Report Access Log](#)
- [Administrator Activities Log](#)

Administrator Report Access Log

The Administrator Report Access Log displays the report access activities performed by Administrators (CSRs) in a given time period. This report displays the following information:

Table 4-2 Administrator Report Access Log fields

Report Field	Description
Issuer Name	The name of the Issuer.
Admin Name	The Administrator's User ID.
Report Type	The name of the report that the corresponding Administrator ran.
Card Number	The card number the Administrator defined when running the corresponding report (not applicable to all reports).
Start Date	The start date of the date range defined by the Administrator when running the report.
End Date	The end date of the date range defined by the Administrator when running the report.
Date Accessed	The date the Administrator ran the report.

To view the Administrator Report Access Log:

1. Click the **Administrator Report Access Log** link.

The *Administrator Report Access* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Administrator Activities Log

The Administrator Activities Log displays information regarding the system activities performed by Administrators in a given time period. This report displays the following information:

Table 4-3 Administrator Activities Log fields

Report Field	Description
Issuer Name	The name of the Issuer.
Admin Name	The Administrator's User ID.
Action	The task performed by the Administrator (for example, Cardholder Account Enquiry)

Table 4-3 Administrator Activities Log fields

Report Field	Description
Cardholder Name	The name of the cardholder associated with the corresponding Action (not applicable to all actions).
Card Number	The card number associated with the corresponding Action (not applicable to all actions).
Date Accessed	The date the action was performed.
Detail	Any system information regarding the action (for example, Admin Logged in Successfully).

To view the Administrator Activities Log:

1. Click the **Administrator Activities Log** link.

The *Administrator Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Issuer Administrator Account Reports

There are two reports that display information about Issuer Administrator system access:

- [Issuer Administrator Report Access Log](#)
- [Issuer Administrator Activities Log Report](#)

Issuer Administrator Report Access Log

The Issuer Administrator Report Access Log displays the report access activities performed by Issuer Administrators in a given time period.

See [Table 4-2 on page 66](#) for descriptions of the information displayed by this report.

To view the Issuer Administrator Report Access Log:

1. Click the **Issuer Admin Report Access Log** link.

The *Issuer Admin Report Access Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Issuer Administrator Activities Log Report

The Issuer Administrator Activities Log displays information regarding the system activities performed by Administrators in a given time period. The report displays the following information:

Table 4-4 Issuer Administrator Activities Log Report

Report Field	Description
Issuer Name	The name of the Issuer
Admin Name	The Issuer Administrator's User ID.
Action	The task performed by the Issuer Administrator (for example, Admin Login).
Date Accessed	The date the task was performed.
Detail	Any system information regarding the action (for example, Admin Logged in Successfully).

To view the Issuer Administrator Activities Log:

1. Click the **Issuer Admin Activities Log** link.

The *Issuer Admin Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Global Administrator Account Reports

Global Administrator Activities Log

The Global Administrator Activities Log displays information regarding the system activities performed by Global Administrators in a given time period. This report displays the following information:

Table 4-5 Global Administrator Activities Log fields

Report Field	Description
Admin Name	The Global Administrator's User ID.
Action	The task performed by the corresponding Global Administrator. (For example, Update FI Information)
Date Accessed	The date the action was performed.

Table 4-5 Global Administrator Activities Log fields

Report Field	Description
Detail	Upon being expanded, displays the details associated with the corresponding Action (for example, parameters changed, messages displayed, and so on).

To view the Global Administrator Activities Log:

1. Click the **Global Admin Activities Log** link.

The *Global Administrator Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Global Administrator Report Access Log

The Global Administrator Report Access Log displays the report access activities performed by Global Administrators in a given time period.

See following table for descriptions of the information displayed by this report.

Table 4-6 Global Administrator Activities Log Report

Report Field	Description
Admin Name	The Global Administrator's User ID.
Report Type	The name of the report that the corresponding Administrator ran.
Start Date	The start date of the date range defined by the Administrator when running the report.
End Date	The end date of the date range defined by the Administrator when running the report.
Date Accessed	The date the Administrator ran the report.

To view the Global Administrator Report Access Log:

1. Click the **Global Admin Report Access Log** link.

The *Global Admin Report Access Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Figure 4-3 Report Access Log

Global Admin Report Access Log

AS OF DATE:2001-10-04 -- 2004-06-29

Run date/time:2004-06-29 11:27:51 PM PST

1

Retrieved:77 Displaying:1 - 77

Admin Name	Report Type	Start Date	End Date	Date Accessed
VGA	GLOBAL_ADMIN_ACTIVITIES_LOG	2001-10-04 12:00:00 AM PST	2004-06-29 11:59:59 PM PST	2004-06-29 11:28:44 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:33:03 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:33:35 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:32:23 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:31:38 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-09-28 12:00:00 AM PST	2004-06-23 11:59:59 PM PST	2004-06-23 04:10:10 AM PST

Figure 4-4 Activities Log

Global Administrator Activities Log

AS OF DATE:2001-10-04 -- 2004-06-29Run date/time:2004-06-29 11:30:56 PM PST

1 2 3 4 5 [Next>>]

Retrieved:404 Displaying:1 - 100

Admin Name	Action	Date Accessed	Detail
VGA	Admin Login	2004-06-29 11:32:38 PM PST	Detail
VGA	Admin Login	2004-06-29 11:32:30 PM PST	Detail
VGA	Admin Login	2004-06-29 11:28:28 PM PST	Detail
VGA	Update FI Information	2004-06-29 10:31:57 PM PST	Detail
VGA	Update FI Information	2004-06-29 10:31:41 PM PST	Detail

Figure 4-5 Activity Details

Global Administrator Activities Log	
AS OF DATE: 2001-10-04 -- 2004-06-29 Run date/time: 2004-06-29 11:32:13 PM PST	
Admin Name	VGA
Action	Admin Login
Date Accessed	2004-06-29 11:32:38 PM PST
Column/Parameter Name	Value
Message	Primary Admin has got privilege from a peer Admin

Administrator (CSR) Operations

Your Issuer's cardholders will contact your applicable customer service department with a variety of service needs related to 3-D Secure enrollment and their secret passwords. For example, cardholders may have difficulty completing a 3-D Secure enrollment, cardholders may forget their secret passwords or want to change their passwords for security reasons, and so on.

This chapter describes the following topics related to managing cardholder enrollment:

- Standard, Abridged and Activation During Shopping (ADS)
- Managing Cardholder Accounts

NOTE:

This chapter describes all possible Administrator privileges. Whether or not you have authority to complete the tasks described is defined by your Issuer Administrator.

About Cardholder Enrollment

This section describes the following cardholder enrollment processes:

- [Standard Enrollment](#)
- [Abridged Enrollment](#)
- [Activation During Shopping \(ADS\)](#)

Standard Enrollment

Many cardholders will enroll in the 3-D Secure program using their Issuer's enrollment Web site. This Web site is part of the Issuer Software and operates without any interaction with the Issuer's Administrators (CSR). This section describes the cardholder's interaction with the system.

There are two steps involved in a standard enrollment:

- [Verifying Cardholder Identity](#)
- [Creating the Cardholder's Identifiers](#)

Verifying Cardholder Identity

The first step in a standard enrollment is verifying the identity of the cardholder that is attempting to enroll in the 3-D Secure program. The Issuer determines its own method of verifying the cardholder. See the *Arcot TransFort Issuer Software Introduction Manual* for detailed information about these verification methods.

During the verification process, the cardholder answers a set of questions related to the cardholder's identity (personal information such as credit card billing address, mother's maiden name, and so on), and about the cardholder's credit history and financial activities. The responses to these questions are verified based on the verification method employed.

Creating the Cardholder's Identifiers

Once the cardholder's identity has been established, the system prompts the cardholder to create a secret password. The cardholder will use this password for all 3-D Secure purchase transactions at participating merchant Web sites.

Next, the cardholder creates a personal message. This message is displayed any time the cardholder makes an online purchase using the 3-D Secure program. This message appears during a purchase transaction and offers the cardholder assurance that the transaction is secure and valid.

The cardholder may also be prompted to create a hint and response, depending on the Issuer cardholder enrollment configuration. The response to the hint acts as a secondary password to identify the cardholder in the event that the cardholder forgets the secret password.

Once the cardholder has been successfully enrolled, the cardholder is free to make purchases on participating merchant Web sites.

Abridged Enrollment

In certain cases, it may be appropriate for you to manually enroll some of your cardholders. This is called an **Abridged Enrollment**, and basically consists of you adding the cardholder's name and card number to the Issuer Software database and giving the cardholder a temporary password to use at your Issuer's Abridged Enrollment Web site. If you manually enroll a cardholder, the cardholder does not have to perform the standard enrollment process and is allowed to perform only a small subset of the steps required to enroll in the 3-D Secure program.

An Abridged Enrollment may be appropriate for cardholders who have had difficulty completing the standard enrollment process. You may also choose to use Abridged Enrollments for your preferred customers (VIPs).

NOTE:

Cardholder identity verification is not enabled in the system for Abridged Enrollments. It is the Issuer's responsibility to verify the identity of cardholder's requesting Abridged Enrollment. For information on your company's policies regarding Abridged Enrollment, see your manager.

For information on how to manually enroll a cardholder, see [“Adding Cardholder Accounts” on page 75](#).

Activation During Shopping (ADS)

An Issuer can automatically enroll cardholders into the online payer authentication program. Issuers can enable ADS in three ways:

1. **Opt-In**
2. **Issuer Activation**

3. Purchase Attempts

These features are described in the section below.

Opt-In

In this method the cardholder is introduced to the online payer authentication program while purchasing at a participating merchant's web site. The cardholder is presented with an opt-in page which may include a temporary password hint. If the cardholder chooses to enroll at this point the password page appears and the purchase transaction continues as a authenticated transaction and the cardholder is auto-enrolled into the program. The cardholder has a choice of opt-in later and the purchase transaction is still completed in this case, but as a non-authenticated transaction. The opt-in page is shown again when the cardholder makes purchases and the number of times this page appears is decided by the Issuer.

Issuer Activation

The cardholder can be forced to enroll into the program by showing the welcome page directly. Also, if the cardholder defers the OptIn feature for a maximum number of times, the number being decided by the Issuer, the Issuer can enforce enrollment of the cardholder. This enrollment is communicated the next time the cardholder attempts a purchase transaction. The cardholder is welcomed into the online payer authentication program and the password page appears. At this point the cardholder is forced to enter the password to complete the transaction. On completing this step, the cardholder the auto enrolled into the program.

Purchase Attempts

The cardholder configured for the Attempts feature is introduced to the virtues of the online payer authentication program. The cardholder information is logged in the Issuer Software Database and the purchase continues as a non-authenticated transaction. This information can be used to spotlight active shoppers over the internet. Such cardholders can be potential candidates for the online payer authentication program. The statistical information can be used as a marketing/sales tool.

You can see the *Arcot TransFort Issuer Software Introduction Manual* for more information about the end user experience during ADS.

Managing Cardholder Accounts

This section provides detailed instructions on how to use the Administrative Console to perform the following cardholder account tasks:

- [Adding Cardholder Accounts](#)
- [Viewing Cardholder Account Information](#)
- [Updating the User ID](#)
- [Locking/Unlocking Cardholder Accounts](#)
- [Viewing the details of a particular cardholder's account](#)
- [Updating Cardholder Enrollment Responses](#)
- [Resetting a Cardholder's Password](#)
- [Cancelling Cardholder Accounts](#)
- [Receiving Promotional Emails](#)
- [View/update Do Not Prompt](#)
- [Changing the Locale of a Card](#)

NOTE:

The procedures in this section assume you are already logged on to the Administrative Console as an Administrator. See [“Logging in and out of the Administrative Console”](#) on page 45 for detailed instructions.

Adding Cardholder Accounts

This function allows you to enroll a cardholder using the [Abridged Enrollment](#) method. To manually enroll a cardholder, complete the required information in the *Add Cardholder* page. Then give the cardholder a temporary password and the URL to your Issuer's Abridged Enrollment Web site. The cardholder will then complete a subset of the enrollment process on this Web site.

The temporary password that you give the cardholder expires after a designated amount of time. For example, your company may require that the cardholder access the Abridged Enrollment Web site and enroll within 48 hours of talking to the Administrator (CSR). This temporary password time limit is configurable, and is set by the Issuer Administrator. For information about configuring temporary password duration, see [“Configuring Issuer Parameters”](#) in [Chapter 6](#).

CAUTION:

Before adding a cardholder using the Abridged Enrollment method, ensure that you know and understand your company's policies regarding this type of enrollment.

To add a cardholder account:

1. Click the **Add Cardholder** link.

The *Add Cardholder* page appears.

2. Enter the card number and click **Submit**.

The page asks for more information.

3. Enter the applicable information in the appropriate fields.

The following table provides detailed descriptions of each field.

Table 5-1 Add Cardholder Fields

Field	Description
Name	The name of the cardholder as it appears on the card.
Password	The temporary password that the cardholder will use to log on to the Abridged Enrollment Web site to complete the enrollment process. You can choose to either enter a password or click the provided link to have the system generate a random password.
Reason	The reason that the cardholder is being manually enrolled. There are two options: Failed User User was unable to complete the standard registration. VIP Registered due to the customer's preferred cardholder status.
Remarks	Additional information regarding the need to perform an Abridged Enrollment for the cardholder or how the cardholder identity was verified.

4. Click **Submit**.

The message "Cardholder <name> added" appears.

Remember to give the temporary password, password duration, and Abridged Enrollment Web site URL to the cardholder once you add the account. If you do not know the default password duration or URL, contact your supervisor.

NOTE:

An Issuer can configure the cardholder enrollment parameters making only the card number mandatory for enrollment. The cardholder name could be an optional field. If you are using such a configuration, leave the Name field empty, and enter only the card number and the temporary password.

NOTE:

You will be unable to view the cardholder you just added in any other tasks or report options except the Cardholders Added by Administrator report until the cardholder completes the enrollment process on your Abridged Enrollment Web site.

Viewing Cardholder Account Information

The Cardholder Account Inquiry function allows you to view the account information of a particular cardholder. This function also provides links to the following cardholder account functions:

- Update the cardholder responses to Issuer questions
- Reset the cardholder's secret password.
- Update The cardholder's User ID
- Cancel the cardholder's 3-D Secure Service
- To allow the cardholder to receive Promotional Emails
- View/Update Do Not Prompt for a cardholder
- To lock/unlock the cardholder from the 3-D Secure Service
- Viewing the details of a particular cardholder's account.
- Changing the locale of a card.

NOTE:

You will be unable to use this function to view information for cardholders who have been added to the system using the Abridged Enrollment process but have not completed the enrollment. To view information for such cardholders, see the *Arcot TransFort Issuer Software Reports Manual*.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number in three tables:

- Enrolled Cardholders - Activated and Pre-Activated
- Pre Enrolled Cardholders
- Cancelled Cardholders

The following tables provides detailed information of the fields in each of the displayed cardholder tables:

Table 5-2 Enrolled Cardholders

Field	Description
Cardholder Name	The name of the cardholder as it appears on the card. This is a link which provides details of the particular cardholder. It also displays the last three 3-D Secure purchase transactions authenticated for the selected cardholder.
Update User ID	This link allows the administrator to update the cardholder's User ID provided he has the privilege to "Reset Password" for the cardholders.
Expiration Date	The expiration date of the card. WARNING This field might not contain a valid value always. It might include the unused constant "2100/12" for cardholders that have enrolled through ADS.
Enabled	This check box indicates if the enrolled card is enabled for the 3-D Secure program.
Reset Cardholder Password	This link allows the administrator to reset the cardholder's secret password. You can reset the passwords of only the Activated cardholders.
Update Cardholder Registration Data	This link allows the administrator to update the cardholders answers to the Issuer's questions.
Cancel 3-D Secure Service	This check box allows the administrator to deactivate the cardholder from the 3-D Secure program.
Receive Promotional Emails	This checkbox is to indicate if the cardholder wants to receive promotional e-mails. The administrator can update this provided he has "Lock/Unlock" cardholder privilege.

Table 5-2 Enrolled Cardholders

Field	Description
Status	This column displays the status of the cardholder. The possible values are: • Activated - which means that the cardholder is enrolled and can perform an authenticated transaction. • Not yet Activated - which means the cardholder is enrolled, but has to complete validation and 'Activate' the account before attempting an authenticated transaction.
Callout Data	This column is populated by callouts. You can display any relevant information passed by the callouts.
Do Not Prompt	The administrator can view/update this option provided he has the privilege to "Cancel Enrollment" for the cardholders.

Table 5-3 Pre Enrolled Cardholders

Field	Description
Cardholder Name	The name of the cardholder as it appears on the card.
Update Cardholder Registration Data	This link allows the administrator to update the pre-enrolled cardholders answers to the Issuer's questions.

Table 5-4 Cancelled Cardholders

Field	Description
Cardholder Name	The name of the cardholder as it appears on the card. This is a link which provides details of the particular cardholder.
Expiration Date	The expiration date of the card you are enrolling.

3. The page displays a **Locale** drop-down box to select any of the Issuer supported locales for the card. The locale is changed for all the cardholders for the card.

The page also displays a **Remarks** text box where the administrator can enter any remarks for the actions performed. You can also choose a **Reason** for cancelling the 3-D Secure service from the drop down box.

Figure 5-1 Cardholder Account Inquiry Page

Cardholder Account Inquiry

This option allows you to make cardholder account enquiry, activate/deactivate a cardholder, reset cardholder's password, update cardholder registration data, cancel "3-D Secure" service and also update User ID if supported.

Card Number: 1000100010001002 Select locale: English-United States ▼

Enrolled Cardholders									
Card Holder Name	Update User ID	Expiration Date	Enabled	Reset Cardholder Password	Update Cardholder Registration Data	Cancel 3-D Secure Service	Receive Promotional Emails	Status	Callout Data
JOHN SMITH	JOHN SMITH		✓	Reset	Update	☐	☐	Activated	null
ANN SMITH	ANN SMITH		✓	Reset	Update	☐	☐	Activated	null

Do Not Prompt: ☐

Reason for cancelling 3-D secure service: Lost/Stolen ▼

Remarks:

Submit
Cancel

Updating the User ID

When a cardholder forgets the User ID or for other security reasons wants to change the User ID, you can update the User ID for the cardholder.

To update cardholder's User ID:

1. Click the **Cardholder Account Inquiry** link. Type the card number in the applicable field and click **Submit**.
2. The system displays the account information for the selected card number in the *Enrolled Cardholders* table.
3. In the **Update UserID** field click on the User Id that you want to change to display *Update User ID* page.
4. Enter a new User ID in the **New User ID** field and click **Submit**.

Locking/Unlocking Cardholder Accounts

When required you can lock or unlock a cardholder account. Locking a cardholder's account temporarily prevents the cardholder from doing 3-D Secure transactions.

To lock/unlock a cardholder account:

1. Click the **Cardholder Account Inquiry** link.
The *Cardholder Account Inquiry* page appears.
2. Type the **card number** in the applicable field and click **Submit**.
The system displays the account information for the selected card number.
3. Do one of the following:
 - a. To lock a cardholder account, clear the **Enabled** check box.
 - b. To unlock a cardholder account, select the **Enabled** check box.You can add any appropriate remarks in the text box provided.
4. Click **Submit**. The system displays the *Cardholder Account Inquiry* page with the message "Locked/unlocked cardholder account successfully."

Viewing the details of a particular cardholder's account

1. Click the **Cardholder Account Inquiry** link.
The *Cardholder Account Inquiry* page appears.
2. Type the **card number** in the applicable field and click **Submit**.
The system displays the account information for the selected card number.
3. To view the details of the selected cardholder account, click on the **cardholder name** in the appropriate section.

The system displays the following details for the cardholder:

- Card Number
- Cardholder Name
- Enabled - a yes/no display to indicated whether cardholder is locked or unlocked

- Enrollment Date
- Date Activated - a timestamp when the cardholder is validated and the status is changed from pre-activated to activated.
- All successful 3-D Secure transactions
- Date on which the 3-D Secure service was cancelled (if cancelled)
- Date on which any cardholder information was updated by the cardholder using the Account Assistant.

NOTE:

This field is updated when a CSR updates the account information or when a cardholder updates account information using the *Update Your Profile* link on the enrollment website.

Updating Cardholder Enrollment Responses

When cardholders enroll in the 3-D Secure program, they may respond to one or more questions regarding their identity, depending on how the Issuer Enrollment site is configured. If requested to do so by a cardholder, you can update the cardholder's responses to these questions. You can update the responses of both enrolled cardholders and pre enrolled cardholders.

To update cardholder's responses:

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

NOTE:

The card number you have entered is displayed in the top left corner of the account information table.

3. Do any one of the following
 - a. Click the **Update** link in the *Enrolled Cardholders* table to update the responses of the particular enrolled cardholder.

- b. Click the **Update** link in the *Pre Enrolled Cardholders* table to update the responses of the particular pre enrolled cardholder

The *Modify Cardholder Responses to Issuer's Questions* page appears. The page displays the card number, cardholder name, the Issuer's questions, and cardholder's responses.

4. Modify the responses, update the **Remarks** field, and click **Submit**.

The system displays the *Cardholder Account Inquiry* Page with the message "Issuer answers have been updated successfully".

Resetting a Cardholder's Password

When a cardholder forgets the secret password or for other security reasons wants to change the secret password, you can create a temporary password for the cardholder. The cardholder can then use the temporary password to change the secret password via the *Forgot your password?* link on the Issuer's Enrollment Web site.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Click the **Reset** link for the particular cardholder in the *Enrolled Cardholders* table.

The *Reset Cardholder Password* page appears and displays the cardholder's name, card number, and card expiration date.

4. Type the **new password** and any **remarks** in the applicable fields.

If you want the system to randomly generate a password, click the **Click here to generate a password** link instead of typing anything in the **Password** field. The system generates a password and populates the **Password** field.

5. Click **Submit**.

The system displays the *Cardholder Account Inquiry* Page with the message "Temporary password created for cardholder <name>" appears. Give the temporary password, password duration, and URL to the 'Forgot your Password?' or 'Reset Password' on the Enrollment Web Site to the cardholder and tell the cardholder to change the password before it expires.

Cancelling Cardholder Accounts

Cancelling a cardholder account removes the 3-D Secure service from the cardholder's account. It does *not* cancel the actual credit card account.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the check box of the **cardholder name(s)** you wish to deactivate and click **Submit**. You can choose a reason for cancelling from the drop-down box provided.

The system displays the *Cardholder Account Inquiry* Page with the message "Cardholder <name> deactivated". The *Cancelled Cardholders* table on the page is updated with this information. Clicking on the cardholder name will display the details of that particular account.

Receiving Promotional Emails

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the check box of the **cardholder name(s)** who wish to receive promotional Emails and click **Submit**.

View/update Do Not Prompt

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the Do Not Prompt check box to indicate that no prompts will be received by the cardholder(s) and click **Submit**.

Changing the Locale of a Card

You can choose the locale of the card from the list of locales which the Issuer supports. This locale becomes the preferred locale for all the cardholders for the given card number. The cardholder can view the CAP pages in this locale.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the preferred locale you want from the drop-down box provided. This is the total list of locales supported by the Issuer.

Click **Submit**. The system displays a message “Locale Changed Successfully”.

Issuer Administrator Operations

Issuer Administrators are responsible for configuring the Issuer accounts in regards to cardholder enrollment in the 3-D Secure program. Issuer accounts are created by Global Administrators. For information on creating Issuer accounts, see [Chapter 5, “Administrator \(CSR\) Operations”](#).

NOTE:

This tasks described in this chapter are privileges of an Issuer Administrator. Whether or not you have authority to complete the tasks described is defined by another Issuer Administrator or your Global Administrator.

This section provides instructions on the following tasks relating to Issuer accounts:

- Configuring Issuer Parameters
- Managing Administrators and Issuer Administrators

NOTE:

The procedures in the following sections assume you are already logged on to the Administrative Console as an Issuer Administrator. See [“Logging in and out of the Administrative Console” on page 45](#) for detailed instructions.

Configuring Issuer Parameters

As an Issuer Administrator, you can configure certain parameters that affect how the Issuer Enrollment Web site performs certain functions and how the Administrative Console is displayed. You can also define the password policy for the Issuer's cardholders.

To configure Issuer parameters:

1. Click the **Configure Issuer Parameters** link.

The *Issuer Configuration Parameters* page appears.

Figure 6-1 Configure Issuer Parameters Screen

Issuer Configuration Parameters	
Configure the appropriate values for the Issuer configuration parameters and click Submit .	
Default Report Display Parameters for Admin	
Date Order for Report Generation	Month, Day and Year ▾
Time Stamp Format in Report	yyyy-MM-dd hh:mm:ss a z ▾
Records Per Page	20 ▾
Admin Display Parameters	
Link to Arcot Home	Yes ▾
Display Arcot Symbol	Yes ▾
Data Upload Parameters	
DU Passphrase	****
Re-type DU Passphrase	****
Cardholder Display Parameters (ACS-CAP)	
Date Format	YY:DD:MM ▾
Date Separator	: ▾
Cardholder Authentication Parameters	
Temp Password Duration	4
Action for Cardholder Authentication after failed login attempts	
Lock Account	☒
Submit Cancel	

2. The following table provides descriptions of the Issuer parameters:

Table 6-1 Issuer Parameters

Parameter	Description
Default Report Display Parameters for Administrative Console	
Date Order for Report Generation	The date order to be used during report generation. The following formats are available: Month, Day and year Year, Month and Day Day, Month and Year
Time Stamp Format in Report	The timestamps format that will be used in system reports. The following formats are available (examples of each shown): yyyy-MM-dd hh:mm:ss a z 2002-08-28 10:38:10 PM GMT MM-dd-yyyy hh:mm:ss a z 08-28-2002 10:38:10 PM GMT MM/dd/yyyy hh:mm:ss a z 08/28/2002 10:38:10 PM GMT
Records Per Page	The default number of records that the system will display on administrator reports.
Administrative Console Display Parameters:	
Display Arcot Symbol	Whether or not the Arcot Systems logo will appear in the Administrative Console.
Link to Arcot Home	Whether or not the Arcot Systems logo is linked to the Arcot Systems home page. This feature is not valid if the Display Arcot Symbol parameter is disabled.
Data Upload Parameters:	
DU Pass Phrase	The passphrase used by the Upload Encryption Tool of the Data Upload Tool to encrypt the Issuer's data during upload. See <i>Arcot Data Upload Tool for Transfort Installation and User Manual</i> for more information.
Cardholder Display Parameters:	

Table 6-1 Issuer Parameters

Parameter	Description																
Date Format	The format that will be used to display the date during purchase transactions. The following date formats are available (examples of each shown): <table> <tr> <td>MM:DD:YY</td><td>08:28:02</td></tr> <tr> <td>DD:MM:YY</td><td>28:08:02</td></tr> <tr> <td>YY:MM:DD</td><td>02:08:28</td></tr> <tr> <td>YY:DD:MM</td><td>02:28:08</td></tr> <tr> <td>MM:DD:YYYY</td><td>08:28:2002</td></tr> <tr> <td>DD:MM:YYYY</td><td>28:08:2002</td></tr> <tr> <td>YYYY:MM:DD</td><td>2002:08:28</td></tr> <tr> <td>YYYY:DD:MM</td><td>2002:28:08</td></tr> </table>	MM:DD:YY	08:28:02	DD:MM:YY	28:08:02	YY:MM:DD	02:08:28	YY:DD:MM	02:28:08	MM:DD:YYYY	08:28:2002	DD:MM:YYYY	28:08:2002	YYYY:MM:DD	2002:08:28	YYYY:DD:MM	2002:28:08
MM:DD:YY	08:28:02																
DD:MM:YY	28:08:02																
YY:MM:DD	02:08:28																
YY:DD:MM	02:28:08																
MM:DD:YYYY	08:28:2002																
DD:MM:YYYY	28:08:2002																
YYYY:MM:DD	2002:08:28																
YYYY:DD:MM	2002:28:08																
Date Separator	Specifies the type of separator that will be used to separate the different elements of the date. The following date formats are available: : / - .																
Cardholder Authentication Parameters:																	
Temp Password Duration	The temporary password duration for the cardholder enrolling through “Abridged Enrollment,” is configured here. This field configures the number of days for which cardholder's temporary password is effective.																
Action for Authentication after failed login attempts	This set of responses specifies how the system reacts to failed login attempts. The Global Administrator specifies the number of login attempts that can be made unsuccessfully. Indicates whether or not the system should lock the cardholder password after a specified number of failed authentication attempts.																
Lock Password																	

- When you have completed your modifications, click **Submit**.

The message “Issuer Configuration Parameters updated” appears.

Managing Administrators and Issuer Administrators

Issuer administrators can perform tasks which manage and control other administrators and Issuer administrators. They can also view the administrator system access reports. This section discusses the following topics:

- Managing Issuer Administrator Accounts
- Managing CSR Accounts
- Viewing Administrator System Access Reports.

Managing Issuer Administrator Accounts

Issuer Administrators create and manage other Issuer Administrators. Issuer Administrators can perform the following tasks associated with managing Issuer Administrator accounts:

- Create Issuer Administrator accounts. See [“Creating Administrators and Issuer Administrators” on page 52](#) for detailed instructions.
- Update administrator privileges for a selected Issuer Administrator. See [“Updating Administrator \(CSR\) and Issuer Administrator Privileges” on page 56](#) for detailed instructions.
- Configure Issuer Administrator password policy. See [“Configuring Administrator Password Policy” on page 60](#) for detailed instructions.
- Enable or disable Issuer Administrator accounts. See [“Enabling/Disabling Administrators” on page 58](#) for detailed instructions.
- Reset Issuer Administrator passwords. See [“Resetting Administrator Passwords” on page 59](#) for detailed instructions.

Managing Administrator (CSR) Accounts

Issuer Administrators can be responsible for creating and managing Administrator accounts. See [“Advanced Authorization” on page 40](#) for more information. You can define a default set of privileges for all Administrators, and adjust the privileges for individual Administrator accounts.

Issuer Administrators can perform the following tasks associated with managing Administrator accounts:

- Create Administrator Accounts. See [“Creating Administrators and Issuer Administrators” on page 52](#) for detailed instructions.
- Update Administrator Privileges for a Selected Administrator. See [“Updating Administrator \(CSR\) and Issuer Administrator Privileges” on page 56](#) for detailed instructions.
- Enable or disable Administrator Accounts. See [“Enabling/Disabling Administrators” on page 58](#) for detailed instructions.
- Reset Administrator passwords. See [“Resetting Administrator Passwords” on page 59](#) for detailed instructions.
- Configure Administrator Password Policy. See [“Configuring Administrator Password Policy” on page 60](#) for detailed instructions.

Viewing Administrator System Access Reports

There are four reports you can use to retrieve and display information about Administrator and Issuer Administrator system use. You can choose to view a report online or export a report to a file to use in another software program.

NOTE:

This section provides instructions on how to view reports online. See [“Exporting a Report to a File” on page 48](#) for instructions on how to export a report.

The system displays reports according to the information set up in your Report Profile. See the [“Updating Your Profile” on page 47](#) for information on how to change your Report Profile.

This section divides the reports into the following categories:

- Administrator (CSR) System Access Reports. See [“CSR System Access Reports” on page 65](#) for detailed instructions.
- Issuer Administrator System Access Reports. See [“Issuer Administrator Account Reports” on page 67](#) for detailed instructions.

Report Codes

This appendix contains the following tables that contain codes listed on the various administrator reports:

- [\\$1Pre-Authorization Response Codes](#)
- [AVS Result Codes](#)
- [CVV/CVC2 Result Code](#)
- [Cardholder Status Code](#)
- [Invalid Request Codes](#)
- [Reason Column Codes for Failed Transactions Report](#)

\$1Pre-Authorization Response Codes

The \$1 Pre-Authorization Response Code is a two-character code that indicates the status or the result of the cardholder's Pre-Authorization screening (also known as \$1 Authorization).

A Response Code of **00** represents a Pre-Authorization approval. A response code of **85** represents a successful card verification. All other response codes represent non-approved requests.

The following table provides descriptions for the Pre-Authorization Response Codes you may see in the Cardholder Enrollment reports:

Table A-1 Pre-Authorization Response Codes

Code	Visa Description	MasterCard Description
00	Approved and completed	Approved and completed
01	Refer to issuer	Refer to issuer
02	Refer to issuer-Special condition	Invalid Merchant
03	Invalid merchant ID	Invalid merchant ID
04	Pick up card	Capture Card
05	Authorization declined	Do not honor
06	General error	--
07	Pick up card-special condition. Response indicates fraudulent use other than lost or stolen.	--
11	Approval; VIP	Approval; VIP
12	Invalid transaction	Invalid transaction
13	Invalid amount	Invalid amount
14	Invalid card number	Invalid card number
15	No such issuer	Invalid Issuer
19	Re-enter transaction	--
30	--	Format Error
39	No credit account	--
41	Pick up card-lost	Lost Card
43	Pick up card-stolen	Stolen Card

Table A-1 Pre-Authorization Response Codes

Code	Visa Description	MasterCard Description
51	Insufficient funds	Insufficient funds
52	No checking account	--
53	No savings account	--
54	Expired card	Expired card
55	Incorrect PIN	Invalid PIN
57	Transaction not permitted to cardholder	Transaction not permitted to issuer/cardholder
58	--	Transaction not permitted to acquirer/terminal
61	Exceeds approval amount limit	Exceeds withdrawal amount limit
62	Restricted card	Restricted card
63	--	Security violation
65	Withdrawal frequency limit exceeded (Activity amount limit exceeded)	--
75	PIN tries exceeded	Allowable number of PIN tries exceeded
76	--	Unable to locate, no match
77	--	Inconsistent data, rev. or repeat
78	--	No account
81	Cryptographic error	--
82	Incorrect Card Verification Value	--
84	Time limit for pre-authorization exceeded	Invalid Authorization Lifecycle
85	No reason to decline	Not declined
86	Unable to verify PIN	--
91	Service unavailable	Authorization System or Issuer System inoperative
92	Routing not successful	Unable to Route transaction
94	--	Duplicate transaction detected
96	--	System error

*. Code not applicable

AVS Result Codes

The AVS Result Code is a one-character code that indicates the result or the status of a cardholder's Address Verification Screening (AVS). The AVS determines the identity of a cardholder based on whether or not the cardholder correctly enters the card billing address when enrolling in the 3-D Secure program.

The following table provides definitions for the AVS Result Codes you may see in the Cardholder Enrollment reports. It also displays the Pre-Authorization Response Code associated with the corresponding AVS Result Code.

Table A-2 AVS Result Codes

AVS Result Code	Description	Pre-Authorization Response Code
A	Address matches but ZIP code does not	00 or 85
E	Error response for Merchant Category code	00 or 85
N	Address and ZIP code do not match	00 or 85
R	Retry; system unavailable or timed out	00 or 85
S	Issuer does not support AVS	00 or 85
U	Address information is not available	00 or 85
W	9-digit ZIP code matches but address does not match	00 or 85
X	Exact match, address and 9-digit ZIP code match	00 or 85
Y	Address and 5-digit ZIP code match	00 or 85
Z	5-digit ZIP code matches, but address does not match	00 or 85
0	Authentication problem	

CVV/CVC2 Result Code

The CVV/CVC2 Result Code is a one-character code that indicates the result or the status of a cardholder's CVV/CVC2 authentication screening. The CVV/CVC2 screening determines the authentication status of a cardholder based on whether or not the cardholder correctly enters a three-digit verification code located on the signature block on the back of the debit or credit card.

The following table provides definitions for the CVV/CVC2 Result Codes you may see in the Cardholder Enrollment reports:

Table A-3 CVV/CVC2 Result Codes

Code	CVV Description	CVC2 Description
M	CVV match	CVC2 match
N	CVV No match	CVC2 No match
P	Not Processed	Not Processed
S	Merchant has indicated that CVV is not present on card	Merchant has indicated that CVC2 is not present on card
U	Issuer is not certified and/or has not provided MasterCard or Visa. encryption keys	Issuer is not certified and/or has not provided MasterCard or Visa. encryption keys

Cardholder Status Code

The Cardholder Status Code is a summary of the state of the cardholder's enrollment authentication. This code is based on the combined status and/or decisions of the authentication methods your Issuer is using for cardholder enrollment.

The following table lists the Cardholder Status Codes that you may find in the Cardholder Enrollment reports:

Table A-4 Cardholder Status Codes

Code	Meaning
\$1_AUTH_FAILURE	The cardholder failed the Pre-Authorization verification check.
\$1_AUTH_SUCCESS	The cardholder passed the Pre-Authorization check, however, the individual aborted the enrollment process before completing it.
ACCEPT_T&C	The cardholder accepted the Terms & Conditions, however, the individual aborted the enrollment process before completing it.
ATTRIBUTES_CALLOUT_FAILURE	Post Verification (Attributes) Step CallOut failed.
ATTRIBUTES_CALLOUT_SUCCESS	Post Verification (Attributes) Step CallOut success.
AVS_FAILURE	AVS verification was unsuccessful.
BAD_RESPONSE_CODE	A Pre-Authorization response code other than 00 or 85 was returned by the AVS verification.
CANCEL_ATTRIBUTES_PAGE	The cardholder cancelled the Attributes Page.
CANCEL_ISSUER_QUESTION	The cardholder cancelled the Issuer QA Page.
CANCEL_PASSWORD_PAM	The cardholder cancelled the Set Password/PAM page.
CARD_HAS_NO_VALID_RANGE	The card number does not belong to any range in the enrollment website.
CH_ABANDONED_ACTIVATION	Cardholder abandoned activation during ADS. No PARes sent.
CH_CANCELLED_ACTIVATION	Cardholder cancelled the activation page during ADS.
CH_DECLINED_ACTIVATION	Cardholder declined to join the online authentication program during ADS.
CVV2/CVC2_FAILURE	CVV2 or CVC2 verification was unsuccessful.

Table A-4 Cardholder Status Codes *(Continued)*

Code	Meaning
DATA_IN_DATABASE	The card number entered was valid, but the cardholder aborted the enrollment process (not an explicit Cancel)
DATA_NOT_IN_DATABASE	The card number was not valid.
DUPLICATE_REGISTER_NO	The cardholder chooses not to re-enroll.
DUPLICATE_REGISTER_REJECT	The Issuer does not allow cardholder re-enrollment
DUPLICATE_REGISTER_YES	The cardholder chose to re-enroll, however, the individual aborted the enrollment process before completing it.
ENROLL_COPY	The cardholder's record is copied to the new card issued to the cardholder. This might be needed in scenarios where one card expires and a new card is issued or the card gets upgraded or side graded. Both the cards might have an overlapping period.
ENROLL_NAME_CHANGE	The cardholder name is changed to a new name. The card number and other details remain the same.
ENROLL_REPLACE	The cardholder's card has been replaced with a new card, for reasons like lost or stolen card.
ENROLLMENT_FAILURE	The cardholder did not successfully complete the enrollment.
ENROLLMENT_SUCCESS	The cardholder successfully enrolled in the 3-D Secure program.
FAILURE_ATTRIBUTES_PAGE	The validation for Attributes Page failed.
GET_QUES_CALLOUT_FAILURE	Pre Verification (Issuer QA) Step callout to get Issuer questions failed.
INVALID_CARD_FOR_RANGE	The card number does not belong to the range in the enrollment website.
ISSUER_QUESTIONS_FAILURE	The cardholder did not answer the Issuer's verification questions correctly.
ISSUER_QUESTIONS_SUCCESS	The cardholder correctly answered the Issuer's verification question, however, the individual aborted the registration process before completing it.
MINI_ENROLLMENT_START	The cardholder started the mini-enrollment.
MINI_ENROLLMENT_SUCCESS	The cardholder successfully enrolled in the 3-D Secure program through mini-enrollment.

Table A-4 Cardholder Status Codes *(Continued)*

Code	Meaning
NO_ISSUER_ANSWERS_IN_DATABASE	Issuer Data policy is >0, but there are no Issuer answers in the Database.
NO_ISSUER_QUESTIONS_IN_DATABASE	Issuer Data policy is >0, but there are no Issuer questions in the Database.
NOT_ACCEPT_T&C	The cardholder did not accept the Terms & Conditions.
PASSWORD/PAM_FAILURE	Cardholder entered account information, however, the individual aborted the enrollment process before completing it.
POPUP_CLOSED	Cardholder closed the popup during ADS. PAREs is sent.
POPUP_TIMEDOUT	The ADS popup is timed out.
POST_FINISH_CALLOUT_FAILURE	After finish callout failed.
POST_MOD1_CALLOUT_FAILURE	Post Identification Step CallOut failed.
PRE_FINISH_CALLOUT_FAILURE	Before Finish callout failed.
QA_CALLOUT_FAILURE	Post Verification (Issuer QA) step callout failed.
QA_CALLOUT_SUCCESS	Post Verification (Issuer QA) step callout success.
SUCCESS_ATTRIBUTES_PAGE	The validation for Attributes Page is successful.
TEMP_PASSWORD_INVALID	Temporary password entered is not correct.
TEMP_RECORD_FOUND	Temporary record for the cardholder found.
TEMP_RECORD_NOT_FOUND	Temporary record for cardholder not found.
AUTO_ENROLLMENT_SUCCESS	The cardholder successfully enrolled into the online authentication program through ADS.
UPLOAD_PREACTIVATED	The cardholder who successfully enrolled into the online authentication program was pre-activated and uploaded using the Data Upload Tool.

PARes Status Code

The possible PARes status codes determined by the ACS are given in the table below:

Table A-5 PARes Status Codes

PARes Status	Description
Y	Authenticated Transaction.
N	Not an authenticated transaction.
U	Unable to authenticate transaction.
A	ACS processing Purchase Attempts of ADS.

ECI Values

The Electronic Commerce Values which will be included in the PAREs if the PAREs status is “Y” or “A” is given in the table below:

Table A-6 ECI Values in PAREs

PAREs Status	Visa ECI value	MasterCard ECI value
Y	05	02
A	06	01

Invalid Request Codes

The IReq code is an error code indicating the particular data which invalidates the VReq. This field is included when the VReq is syntactically correct, but business processing cannot be performed for some reason identified by the code. The following table lists and describes the Ireq codes.

Table A-7 Invalid Request Codes

Code	Description
50	Acquirer not participating in 3-D Secure.
51	Merchant not participating in 3-D Secure.
52	Password required, but no password was supplied.
53	Supplied password is not valid for combination of Acquirer BIN and Merchant ID.
54	ISO code not valid per ISO tables (for either country or currency).
55	Transaction data not valid. For example: • purchase amount is not the same as display amount • PAREq.acctid is not the same as VERes.acctid
56	PARReq was incorrectly routed; either: • the PARReq was received by the wrong ACS, or • the PARReq should never have been sent, based on the values in the VERes.
57	Serial number cannot be located
98	Transient system failure
99	Permanent system failure

Reason Column Codes for Failed Transactions Report

The Reason column in the Failed Transactions report summarizes the reason for the failure. The table below lists and describes the reasons:

Table A-8 Reason for Failed Transactions

Reason	Description
AAV_HMAC_ERROR	AAV generation failed.
AAV_HMACKEY_ERROR	HMAC key not found or key is invalid.
ARQC_ERROR	Chip card error.
ATTEMPTS	Attempts Transaction
AUTH_FAILED	Cardholder failed authentication.
CALLOUT_ABORT	The callout invoked was aborted.
CANCEL	Cardholder cancelled the transaction.
CARD_EXPDATE_DECRYPT_ERROR	Error while decrypting card expiry date.
CAVV_GEN_ERROR	CAVV generation failed.
CAVV_KEY_ERROR	CVV key pairs not found or key pair is invalid.
CH_DATA_ERROR	Cardholder data exceeding in memory buffer.
CH_LOCKED	The cardholder was locked during the transaction.
CH_NAME_DECRYPT_ERROR	Error while decrypting cardholder name.
CH_NAME_ENCRYPT_ERROR	Error while encrypting cardholder name.
CH_NAME_UPDATE_FAILED	Cardholder name could not be updated due to Update Cardholder Profile callout error.
CH_NOTFOUND	Mismatched account.
CH_REENROLL	The cardholder wants to add a secondary cardholder through the Welcome page and there is no Verify Issuer Answers Callout configured.
CH_STATUS_INVALID	Cardholder's status not valid for transaction.
CVV_KEYIND_INVALID	Invalid CVV Key indicator value

Table A-8 Reason for Failed Transactions

Reason	Description
DATABASE_FAILURE	Could not connect to database.
HINT_FAILED	Cardholder failed authentication during Hint/Response.
INVALID_PROXYPAN	Cardholder proxy pan not valid.
NO_VIA_CALLOUT	VIA CallOut is required but is not configured. For example, If you want to enroll secondary cardholder, the VIA callout is mandatory.
OPTIN_DECLINE	Cardholder declined to join the online authentication program during ADS.
OPTIN_POPUP_CLOSED	Cardholder closed the popup during ADS.
OPTIN_POPUP_TIMEDOUT	The popup during ADS was timed out due to cardholder inactivity.
PAN_DECRYPT_ERROR	Error while decrypting cardholder PAN.
PARAQ_CALLOUT	The status of the transaction as decided by the PAREq callout. This is used to implement Advanced ADS.
PARAQ_MATCH_FAILED	PARAQ did not match/have corresponding VEReq. Can be a case of a replay attack.
PARAQ_VALIDATION_FAILED	PARAQ does not conform to the 3-D Secure specifications.
PARES_GEN_FAILED	Error in generating PAREs XML message.
POPUP_CLOSED	Cardholder closed the popup during transaction. PAREs was sent.
POPUP_TIMEDOUT	Cardholder's popup is timed-out due to inactivity.
PRE_PARES_CALLOUT	The status of the transaction as decided by the Pre PAREs callout. This is used to implement Advanced ADS.
RCPT_FAILED	Receipt failed.
SEC_CH_INSERT_FAILED	Secondary cardholder could not be inserted.
SET_PWD_FAILED	Cardholder could not set the secret password.
SIGNPARES_FAILED	Invalid signing certificate for range.
TX_DBINSERT_FAILED	Database flush failed.

Error Codes

This appendix contains the following tables that list the error codes that are found in the Access Control Server (ACS) component of the Issuer Software:

- Transaction Detail Status Codes
- Processing Errors

If you experience problems with the Arcot Issuer Software, you should contact Arcot Customer Support.

Arcot Customer Support: 1.408.969.6250

Transaction Details Status Codes

Table B-1 Transaction Details Status Codes

Status Codes	Description
000	Core Payer Authentication successful.
001	Core Payer Authentication cancelled on Password page.
002	Core Payer Authentication failed.
003	Core Payer Authentication cancelled on Hints page.
011	Core Payer Authentication failed. ACS database error.
020	Core Payer Authentication failed. ACS Web interface error.
030	Core Payer Authentication failed. Directory Server system error.
031	Core Payer Authentication failed. Directory Server database error.
040	Core Payer Authentication failed. MPS system error.
050	Core Payer Authentication failed. Verification Server system error.
100	Chip Card Authentication successful.
101	Chip Card Authentication failed. No ARQC generated.
102	Chip Card Authentication failed. ARQC could not be validated.
103	Chip Card Authentication failed. No eAccess application found on card.
104	Chip Card Authentication failed. Installed software faulty.
110	Chip Card Authentication failed. ACS system error.
120	Chip Card Authentication failed. ACS Web interface error.
130	Chip Card Authentication failed. Directory Server system error.
140	Chip Card Authentication failed. MPS system error.
150	Chip Card Authentication failed. Verification Server system error.
160	Chip Card Authentication failed. Secret password not valid.
170	Chip Card Authentication failed. General failure caused by secret password.
199	Chip Card Authentication failed. General failure.
200	Token Card Authentication successful.
201	Token Card Authentication cancelled on the Password page.

Table B-1 Transaction Details Status Codes

Status Codes	Description
202	Token Card Authentication failed. Token PIN not valid.
210	Token Card Authentication failed. ACS system error.
213	Token Card Authentication failed. Authentication Server not available.
214	Token Card Authentication failed. Challenge not returned by the Authentication Server.
220	Token Card Authentication failed. ACS Web interface error.
230	Token Card Authentication failed. Directory Server system error.
240	Token Card Authentication failed. MPS system error.
250	Token Card Authentication failed. Verification Server system error.
800	ArcotID Authentication successful.
802	ArcotID Authentication failed. ArcotID PIN not valid.
810	ArcotID Authentication failed. ACS system error.
813	ArcotID Authentication failed. Arcot Authentication Server is not available.
814	ArcotID Authentication failed. Challenge not returned by the Arcot Authentication Server.
820	ArcotID Authentication failed. ACS Web interface error.
830	ArcotID Authentication failed. Directory Server system error.
840	ArcotID Authentication failed. MPS system error.
850	ArcotID Authentication failed. Verification Server system error.

Processing Errors

Table B-2 Processing Errors

Error Code	Description
1000	ACS error. ACS was unable to verify enrollment.
1001	ACS error. Password screen could not be constructed.
1002	ACS error. An error occurred while verifying the cardholder's password.
1003	ACS error. Cannot retrieve hint question.
1004	ACS error. Cannot verify answer for the hint question.
1005	ACS error. PAREs generation error.
1006	ACS error. PAREs signing error.
1007	ACS error. Receipt generation error.
1008	ACS error. Receipt saving error.
1009	ACS error. Cannot verify card range.
1010	ACS error. Invalid request message.
1011	ACS error. No ACS database connection available.
1012	ACS error. Daughter window session time-out.
1013	ACS error. Receipt queue is full.
1014	ACS error. Credit card has expired.
1015	ACS error. Arcot Authentication Server is not available.
1016	ACS error. Cannot verify secret associated with the Chip Card.
1017	ACS error. Host security module box is down.
1018	ACS error. The HSM verify ARQC failed.
1019	ACS error. The ACS Client timed out.
1020	ACS error. Invalid Currency Code.
1021	ACS error. Invalid Country Code.
1022	ACS error. Amount and Purchase Amount mismatch.
1023	ACS error. Invalid end recurring payment date format.
1024	ACS error. Invalid card expiration date format.
1025	ACS error. Invalid end recurring payment date.

Table B-2 Processing Errors

Error Code	Description
1026	ACS error. Invalid VEReq extension critical value.
1027	ACS error. Cannot handle VEReq extension element.
1028	ACS error. Invalid PAREq extension critical value.
1029	ACS error. Cannot handle PAREq extension element.
1030	ACS error. ACS operation failed.
1031	ACS error. ACS transport exception thrown.
1032	ACS error. ACS Client read error.
1033	ACS error. ACS shutdown initiated from Admin.
1034	ACS error. ACS_DECRYPTION_ERROR, Crypto Error.
1035	ACS error. ACS_ENCRYPTION_ERROR, Crypto Error.
1036	ACS error. ACS_BAD_SESSIONID_ERROR, bad session id
1037	ACS error. ACS_NO_AHAREC_ERROR, no CH data in AHA table
1038	ACS error. ACS_BAD_RANGE_ERROR, no brandinfo or range info
1998	ACS error. Unknown exception.
1999	ACS error. Last error.
2000	CAP error. Client authentication pages unable to connect to the ACS.
2001	CAP error. User pressed Cancel during Password Request phase
2002	CAP error. User pressed Cancel during hint answer request phase
2003	CAP error. User failed to supply correct hint answer
2004	CAP error. No Challenge returned by Arcot Authentication Server
2005	CAP error. Unable to connect to Arcot Authentication Server
2006	CAP error. User failed to supply EAccess Password
2007	CAP error. No VSDC Data returned from Chip Card Reader
2008	CAP error. No Authentication methods for card number
2009	CAP error. No Chip Card Plug-in on client computer
2010	CAP error. No EAccess Present
2011	CAP error. User Account has been disabled as Bank's PasswordUsagePolicy is 1
6000	Failed to get a merchant data string.

Table B-2 Processing Errors

Error Code	Description
6001	The merchant did not set an authorized purchase amount.
6002	The authorized amount contains characters other than numbers.
6003	The authorized amount is more than 12 characters in length.
6004	The authorized amount is 0.
6006	Missing country code.
6007	The country code contains characters other than numbers.
6008	The country code is not three characters in length.
6011	Missing currency code.
6012	The currency code contains characters other than numbers.
6013	The currency code is not three characters in length.
6016	The transaction date is missing.
6017	The transaction date contains characters other than numbers.
6018	The transaction date is not 6 characters in length.
6019	The date is invalid.
6021	The amount other value is missing.
6022	The amount contains characters other than numbers.
6023	The amount is longer than 12 characters in length.
6024	The amount other value is greater than 0. In Internet transactions, the amount other value must be 0.
6026	Missing XID.
6027	The XID contains characters other than hexadecimal numbers. hexadecimal numbers include: 0123456789abcdefABCDEF.
6028	XID is not 28 or 40 characters in length.
6029	XID base64 decoding failed.
6030	Base64 decoding did not return 20 characters as expected.
6035	Cannot call GetVSDCData() before calling SetMerchantData().
6040	Cannot call GetChipCardSecret() without the PIN.
6041	Could not load the eAccess wallet dll.

Table B-2 Processing Errors

Error Code	Description
6042	Could not call GetProcAddress() on GetSecretFromLibrary(), which retrieves the e-access secret password.
6043	Multiple instances of the browser have multiple instances of the chip card plug-in, and therefore the card was blocked by a mutex.
8000	HTTP Action is not 'POST'.
8001	Invalid HTTP header Content-Type.
8002	Invalid HTTP header Content-Length.
8003	HTTP Response is not 200 OK.
8004	Invalid HTTP Request header has been received.
8005	Invalid HTTP Response header has been received.
8006	No HTTP header Content-Length.
8007	Invalid XML message format.
8008	XML Message Root is not 3-D Secure.
8009	Invalid XML Element.
8010	Server and Client Protocol mismatch.
8011	Invalid Extension Critical value.
8012	Unable to handle Extension Element.
8999	Last XML error.

Glossary

3-D Secure Protocol	An Internet-based protocol used to implement the MasterCard or Visa. Authenticated Payment Program for cardholder authentication (or identification) during an online purchase transaction.
AAV	Account Holder Authentication Value. Cardholder authentication data required by MasterCard for online transactions in which cardholder authentication has been successfully performed.
Abridged Enrollment	An Enrollment process that is used when cardholders are unable to enroll in the 3-D Secure program on their own. Alternatively, Issuers may choose to use this process for VIPs. The process is as follows: An Administrator manually adds a cardholder to the Issuer Software Database and gives the cardholder a temporary password to the Abridged Enrollment Web site. The cardholder accesses the Abridged Enrollment Web site and completes the Abridged Enrollment.
Acquirer	A MasterCard or Visa. Member financial institution that establishes a contractual service relationship with a merchant for the purpose of accepting MasterCard or Visa. cards. In 3-D Secure, determines whether merchant is eligible to participate. Performs traditional role of receiving and forwarding authorization and settlement messages (enters transaction into interchange).
ACS	The Access Control Server (ACS) is the component of the Issuer Software that enables verification of the identity of cardholders enrolled in the 3-D Secure program.
Admin Message Handler	Handles administration messages for the ACS from the ACSClient (regarding, for example, graceful shutdown or refreshing tables).
Administrative Console	Used by the different levels of Issuer Software administrators to perform system administration and cardholder management functions.

Administrator	This level of Issuer Software administrator is also known as a Customer Support Representative (CSR). An Administrator is responsible for administrative activities involving cardholders.
ADS	Activation During Shopping. A method of automatically enrolling cardholders while shopping, into the online authentication program.
Advanced Authorization	A feature for the administrators of the Issuer Software where one level of administrator can have extended functionality of administrators of lower levels.
AHS	The Authentication History Server (built and hosted by MasterCard or Visa.) stores a record for every attempted cardholder authentication by an ACS. Data includes the originating merchant requests and the authentication results.
ArcotIDs	Software smart cards that allow hardware level authentication in software form.
Attributes Step	A step in the ES where the cardholder provides personal information like name, date of birth, etc. during enrollment.
Authenticated Transaction	A e-commerce purchase where the cardholder is verified according to the 3-D Secure protocol to use the payment card.
Authentication	The process of verifying that the person making an e-commerce purchase is entitled to use the payment card.
Authorization	A process by which an Issuer, or a processor on the Issuer's behalf, approves a transaction for payment.
Auto FYP	A feature where the FYP feature is enabled automatically.
AVS	The Address Verification Service determines the identity of a cardholder based on whether or not the cardholder correctly enters the card billing address when enrolling in the 3-D Secure program.
BIN	Bank Identification Number. The first six digits of a payment card account number that uniquely identify the issuing financial institution.
CA	The Certificate Authority refers to the trusted entity that signs, issues, and revokes digital certificates.
CallOut	CallOuts are customized pieces of code that can be invoked for pre-defined events in the ACS and ES.
CAP	The Client Authentication Pages act as a user interface to the ACS. It displays a password pop-up page to cardholders who initiate 3-D Secure purchase transactions at participating merchant sites.
CAP Message Handler	Handles messages for the ACS from the CAP.

Cardholder	Party that holds a payment card, shops, provides card number and commits to payment.
CAVV	Cardholder Authentication Verification Value. A cryptographic value generated by the ACS to provide a way during authorization to rapidly validate the integrity of certain values copied from the Payer Authentication Response to the authorization request and to prove that authentication occurred.
certificate	A specially formatted block of data that contains a public key and the name of its owner. The certificate carries the digital signature of a CA to authenticate it.
certificate chain	An ordered grouping of digital certificates, including the Root certificate, that are used to validate a specific certificate.
chip card	A payment card with an integrated circuit chip that stores information about the account and user.
CVK	A Card Verification Key is a data-encrypting key in the HSM that is used to generate and verify card information (CVV output).
CVV	The Cardholder Verification Value is a verification algorithm used by the HSM to calculate CAVVs, or it can be the results of applying that algorithm to a particular card.
CVV2/CVC2	The Cardholder Verification Value 2 (CVV2) or the Cardholder Validation Code (CVC2) option determines the authentication status of a cardholder based on whether or not the cardholder correctly enters a three-digit verification code located on the signature panel on the back of the card.
DES	Data Encryption Standard is a publicly known cryptographic algorithm that converts plaintext to ciphertext using a 56-bit symmetric key.
digital certificate	See <i>certificate</i>
digital signature	An asymmetric cryptographic method whereby the recipient of the data can prove the origin and integrity of data, thereby protecting the sender of the data and the recipient against modification or forgery by third parties and the sender against forgery by the recipient.
DS	The Directory Server holds records of all card number ranges (but not individual card numbers, the names of the cardholders, or any other personal data) that are enrolled in the 3-D Secure program. It directs authentication requests from the Merchant Software to the ACS responsible for the account information for the cardholder being authenticated.
DS Message Handler	Handles messages for the ACS from the DS.

Dual Control	A feature that requires two administrators to log on to the Administrative Console to perform a specific task.
Enhanced Global Administrator	A global administrator having Advanced Authorization enabled. It means that a global administrator can have privileges of Issuer Administrators and CSR's.
Enrollment	The act of registering cardholders into the MasterCard or Visa. Authentication Payment Program.
ES	The Enrollment Server is the Issuer Software component used to enroll cardholders in the MasterCard or Visa. Authentication Payment Program.
External Verification	Cardholder identity verification during enrollment that is conducted by an Issuer's own authentication system.
FI	In terms of the Issuer Software, Financial Institution refers to the establishment responsible for facilitating customer-initiated transactions for the extension of credit. Also referred to as an Issuer.
FYP	Forgot You Password - a feature where the cardholder can have alternate methods of authentication when the actual password is forgotten.
Global Administrator	An Issuer Software administrator responsible for setting up Issuer accounts and configuring the Issuer Software.
Hardware Accelerator	A hardware component used by the Issuer Software to store Master Keys, Issuer Encryption Keys, and Signing Keys and to perform cryptographic calculations involving those keys.
Hint Question/Answer	Hint is a question configured by the cardholder, which can be used when the cardholder clicks on FYP. The answer is also set by the cardholder.
HMAC	The Keyed-Hash Message Authentication Code is an option for Issuers to use to calculate CAVVs and AAV's.
HSM	The Host Security Module is used by the Issuer Software to enable CVV calculations and chip card support.
Identification Step	The first step in the enrollment process in the ES. This is the step where the cardholder provides the card number.
In Wallet Score	A numerical score between 1 - 999 issued by a third-party authentication service that indicates the cardholder's authentication status.
Internal Verification	Cardholder identity verification during enrollment that is conducted against the Issuer Software Database.
IPGS	The Internet Payment Gateway System processes payment authorizations for online purchases.
Issuer	In terms of the Issuer Software, Issuer refers to the establishment responsible for facilitating customer-initiated transactions for the extension of credit. Also referred to as Financial Institution.

Issuer Administrator	An Issuer Software administrator responsible for managing Administrator accounts, managing other Issuer Administrator accounts, and for configuring Issuer-specific enrollment parameters.
Issuer Encryption Keys	Triple DES keys used to encrypt and decrypt data for the different Issuers hosted by the Issuer Software.
Issuer Questions	Issuer configured questions to verify the cardholder before authentication. Standard questions include asking for the cardholder's mother's maiden name, city of birth, and so on.
Issuer Software Database	The persistent database storage that contains all the data required by an installation of the Issuer Software. This includes cardholder data as well as some component configuration information.
LMK	The Local Master Keys are DES or triple DES keys that encrypt the keys stored on the HSM.
Master Administrators	A pair of Issuer Software administrators who initialize the Issuer Software after installation and set up the first Global Administrators.
Master Key	A triple DES key that is used to encrypt values such as the Issuer Encryption Key labels, the Issuer Software Database user name and password, and so on. There is only one Master Key per Issuer Software deployment.
MDK	The Master Derivation Key on the HSM is used to enable chip card support. In the Issuer Software, this value is referred to as the HSM Variant.
merchant	Entity that contracts with an Acquirer to accept MasterCard or Visa. cards. Manages the online shopping experience with the cardholder, obtains card number, then transfers control to the Merchant Server Plug-in, which conducts payment authentication.
Merchant Server	The Merchant Server handles inter-component messaging between the Merchant Software and the other components in the 3-D Secure system.
Merchant Software	The Merchant Software plugs into the Web Server and is used to trap purchase requests. This is also known as the Merchant Filter or Merchant Plug-in. The Merchant Software also includes an SDK.
nCipher PIN	The operator pass phrase for an operator card included in the nCipher security world used by the Issuer Software. Each operator card in the nCipher security world may have a different PIN.
On-Behalf-Of Host	A third-party organization that hosts the Issuer Software for Issuers.
Online Authentication Program	A method which verifies and authenticates a online transaction in compliance to the 3-D Secure protocol.

Online Payer Authentication Program	One of the programs of the MasterCard or Visa Secure e-Commerce Initiative, this program includes two authentication protocols: 3-D Secure and 3-D SET
Out Wallet Score	A percentage score issued by a third-party authentication service that indicates the percentage of third-party enrollment questions the cardholder answered correctly.
PAN	The Primary Account Number is the number on the payment card that identifies the cardholder's account.
PAReq	The Payer Authentication Request is triggered by a positive response from the ACS regarding cardholder status. This message is sent by the Merchant through the cardholder's browser to the ACS.
PARes	The Payer Authentication Response is a message generated by the ACS in response to a PAReq. Regardless of whether authentication is successful, the ACS generates a PARes message and signs it with its MasterCard or Visa.-branded signing certificate, then sends the message back to the Merchant Software through the cardholder's browser.
Passphrase	The encryption/decryption key used to encrypt/decrypt data during upload.
Pre- Authorization	Pre-Authorization program (also known as \$1 authorization) determines the authentication status of a cardholder based on whether or not a one dollar test purchase authorization is accepted by the cardholder's credit card account.
ProxyPAN	A unique identifier of the card number. This is the value sent in all the external communications instead of the actual card number. The value generated here is always the same for a card number.
Receipt	A receipt is an acknowledgment of an authenticated online payment
Re-enrollment	An alternate method of verifying the cardholder other than password. You can use this method to verify and then allow them to reset the password.
RSA	The Rivest-Shamir-Adleman method is the most commonly used public key algorithm for encryption and digital signatures.
Servlet Container	The Issuer Software uses the Tomcat servlet container to invoke the Enrollment Server and Administrative Console.
Servlet Redirector	A Web server filter that directs requests or user input from a browser to the servlet container and returns content to the browser. The Servlet Redirector directs both cardholder enrollment input and Administrative Console input to the servlet container.
Signing Keys	Private RSA keys used by the ACS to sign Payer Authentication Responses (PARes).

SSL	Secure Sockets Layer. A cryptographic protocol to confidentially transmit information over open networks like the Internet.
Third-Party Verification	Cardholder identify verification during enrollment that is conducted by a third-party such as Experian.
Transaction ProxyPAN	Another identifier for the card number. There is a unique value generated for every transaction.
Verify Enrollment Request	<i>VEReq.</i> Message from MasterCard or Visa. Directory to ACS, asking whether authentication is available for a particular card number.
Verify Enrollment Response	<i>VERes.</i> Message from ACS or MasterCard or Visa. Directory, telling whether authentication is available.

Index

Symbols

- \$1 Pre-Authorization
 - about 13

Numerics

- 3_D Secure
 - about 8
- 3-D Secure
 - cardholder enrollment in. *See* Enrollment

A

- Abridged Enrollment 73
- Abridged Registration
 - temporary password duration 90
- Access Control Server. *See* ACS
- ACS
 - about 10
 - list of processing error codes for 110–113
 - list of transaction details status codes for 108–109
- adding
 - cardholder accounts 75–77
- Address Verification Screening. *See* AVS
- Administrative Console
 - basic tasks 45–48
 - logging in 45–46
 - logging out 46
 - user interface 43–44
- Administrator
 - about 36
 - logging out of Admin Console 46
- Administrator accounts
 - configuring privileges for 62
 - creating 52
 - enabling or disabling 58

- specifying password policy for 60–61
 - updating privileges for 56
- Administrator Activities Log 66–67
- administrator group hierarchy 34–42
- Administrator Report Access Log 66
- administrator, common
 - changing password 46–47
 - dual control 41
 - exporting reports to file 48–49
 - password policies 42
 - privileges 41
 - updating report profile 47
- Auto Enrollment 73
 - Issuer Activation 74
 - Optin 74
 - Purchase Attempts 74
- AVS
 - about 14
 - Result Code table 96

C

- cancelling cardholder accounts 84
- cardholder accounts
 - adding 75–77
 - cancelling 84
 - lock/unlock 81
 - resetting passwords 83
 - updating responses to Issuer questions 82
 - viewing information 77
- cardholder enrollment. *See* Enrollment
- cardholder password
 - temporary password duration 90
- cardholder password policy
 - temporary duration 90
- Cardholder Status Codes 98–99
- Cardholder User Interface

- Account Management 26
 - Cancel Enrollment 29
 - Resetting password 26
 - Transaction History 28
 - Update Profile 29
- Enrollment 18
 - Attributes Step 22
 - home page 18
 - Identification Step 21
 - landing page 18
 - Q&A Step 23
 - Set Password Step 24
 - Set Personal Message step 25
 - T&C Step 21
- Enrollment Sessions 30
- Merging Enrollment steps 30
- Transactions 31
 - ADS 32
 - locale settings 31
- cardholder verification methods 13–14
 - \$1 Pre-Authorization 13
 - external verification 14
 - internal verification 13
- configuring
 - Enrollment Server Parameters for Issuer 88–90
 - Global Administrator privileges 62
- Configuring Issuer Parameters 88–90
- creating
 - Administrator accounts 52
 - Global Administrator accounts 53–54
- CSR Administrator. *See* Administrator
- CSV report format 48–49
- CVV2
 - Result Code table 97
- CVV2/CVC2
 - about 14

D

- date separators, defining 90
- Directory Server
 - about 10

- disabling
 - Administrator accounts 58
- dual control
 - about 41
 - logout secondary 46

E

- ECI Values 102
- enabling
 - Administrator accounts 58
- Enrollment
 - Abridged 73
 - Auto 73
 - Cardholder User Interface 18
 - Standard 72–73
 - transactions 11–12
- Enrollment Server. *See* ES
- error codes
 - processing errors 110–113
 - transaction details status codes 108–109
- ES
 - about
 - exporting reports to file 48–49
 - external verification
 - about 14

G

- Global Administrator
 - about 35
 - logging in to Admin Console 45
 - logging out of Admin Console 46
- Global Administrator accounts
 - creating 53–54
- groups, administrator 34–42

I

- internal verification 13
- Issuer
 - selecting preferred locale 85

Issuer account 88–90

Issuer Administrator

about 35

logging in to Admin Console 45

logging out of Admin Console 46

Issuer Administrator Activities Log 68

Issuer questions 13

updating cardholder responses to 82

Issuer Software Database

about 10

L

lock cardholder 81

lock password, defining for cardholder authentication 90

logging in to Administrative Console 45–46

logging out

of Administrative Console 46

of dual control tasks 46

M

managing

cardholder accounts 75–85

Global Administrator accounts 63–64

Master Administrator

about 34

logging in to Admin Console 46

logging out of Admin Console 46

Merchant Software

about 10

Multiple Locale

Setting Preferred Locale for a Card locale

Setting Card Locale 85

O

on-behalf-of host 9

P

PARes Status Code 101

password policy

about 42

specifying for Administrators 60–61

passwords, administrator

changing own 46–47

passwords, cardholder

resetting 83

temporary 75

personal message 73

Pre-Authorization

Response Code table 94–95

privileges, administrator

about 41

configuring for 62

updating for an Administrator 56

updating for Global Administrator 56

processing error codes 110–113

purchase transactions

process 14–16

viewing for cardholder 77

R

records per report page 47, 89

Registration. *See* Enrollment

report codes

AVS Result Codes 96

Cardholder Status Codes 98–99

CVV2 Result Codes 97

Pre-Authorization Response Codes 94–95

report profile, updating administrator 47

reports

Administrator Activities Log 66–67

Administrator Report Access Log 66

defining time stamps for 89

exporting to file 48–49

Global Administrator Report Access Log 69

Issuer Administrator Activities Log 68

Issuer Administrator Report Access Log 67

resetting

- cardholder passwords 83
- response codes, Pre-Authorization 94–95
- result codes
 - AVS 96
 - CVV2 97

- Global Administrator Reports
 - Global Administrator Activities Log 68
 - Issuer Administrator Report Access Log 67
 - Issuer Administrator reports 65–68, 92

S

- SecureCode
 - components 9–10
 - removing from cardholder account 84
 - transactions 11–16
- specifying
 - Administrator password policy 60–61
- Standard Enrollment 72–73
- status codes
 - cardholder 98–99
 - transaction details 108–109

T

- temporary cardholder passwords 75, 83
- temporary password duration 90
- timestamps
 - authentication transactions 90
 - in reports 89
- transaction details status codes 108–109
- Transactions
 - Cardholder User Interface 31

U

- unlock cardholder 81
- updating
 - Administrator Privileges for an Administrator 56
 - privileges for a Global Administrator 56

V

- viewing
 - cardholder account information 77
 - Global Administrator Report Access Log 69